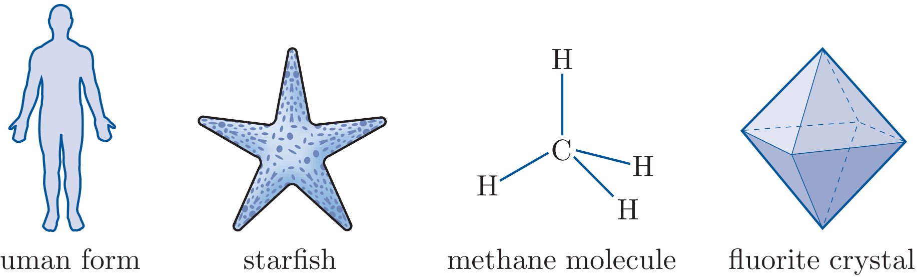
Unit B1

Symmetry and groups

Introduction to Book B

In this book and Book E you will study a branch of mathematics known as *group theory*. The word *group* describes a particular type of mathematical structure that occurs naturally in many branches of mathematics, as well as in other disciplines such as chemistry and physics. In particular, this structure is to be found wherever *symmetry* exists. Figure 1 illustrates some of the many ways in which symmetry occurs in nature: for example, the human form is (outwardly) symmetric, as are many biological, chemical and geological forms.



human form starfish methane molecule fluorite crystal

Figure 1 Symmetry in nature

You will see how groups arise from symmetry, and how they occur in other contexts, such as in relation to addition and multiplication of numbers. You will study the theory of groups, which allows us to discover and make use of the properties of groups that arise from their structure, rather than from the nature of the actual objects that form the group – these objects might be numbers, or functions, or any of many other possibilities. You will see how group theory, a rich and beautiful mathematical theory, is built up from just four simple assumptions about the nature of the structure that we call a group; these assumptions are known as the *group axioms*.

This first book of group theory introduces the basic ideas leading up to a simple but powerful result known as *Lagrange's Theorem*, which underpins much of the development of the subject. The second book of group theory, Book E, takes the theory further. Although you will be learning abstract theory throughout the group theory books, you will also encounter many concrete examples of groups and see how these illustrate the abstract ideas.

The first two units in Book B, namely Unit B1 *Symmetry and groups* and Unit B2 *Subgroups and isomorphisms*, are quite substantial, and you should expect to spend longer studying them than you would for an average unit, particularly for Unit B1. In compensation, Unit B3 *Permutations* and Unit B4 *Lagrange's Theorem and small groups* are shorter.

A note about proofs

In this book, and throughout the rest of this module, you will see many proofs. You have seen some already in previous units, but the number of proofs will increase from now on.

These proofs are important: proofs are an essential part of mathematics. If you take the time to read and understand them, then they will often improve your understanding of the theory, and they will also help you to learn how to write your own proofs, which you are asked to do in some exercises.

However, some proofs can be difficult and time-consuming to read. Also, sometimes a proof may not contribute significantly to your understanding of the theory: for example, it might mostly depend on ideas that are not closely connected to the mathematics that you are currently studying, or it might consist of a largely technical and not very enlightening check through various possible cases. It may be better for you to skip such proofs, at least initially, especially if you are short of time or if you do not plan to go on to study more pure mathematics after M208. Throughout the module, the unit texts provide guidance about some proofs that you might choose to skip or delay reading for these reasons.

Introduction

In this first unit of group theory you will look at ideas of symmetry for two- and three-dimensional shapes, and see how these ideas can be expressed mathematically. You will see how this leads to the concept of a group, and you will meet many other examples of groups. You will also see how some simple results about groups can be deduced directly from the group axioms.

Remember that this is quite a substantial unit, so you should expect it to take more time than an average unit.

1 Symmetry in $\mathbb{R}^2$

This first section is about the symmetry of two-dimensional shapes.

1.1 Symmetries of plane figures

When you think of symmetry, you probably think of shapes like the heart shape in Figure 2: it has *reflectional symmetry* because a reflection in its *axis of symmetry* leaves the shape looking the same. Another type of symmetry is exhibited by the capital N also shown in Figure 2: it has *rotational symmetry* because a rotation of a half-turn about its centre leaves the shape looking the same. For other shapes, rotational symmetry may involve a quarter-turn or a third of a turn, for example.

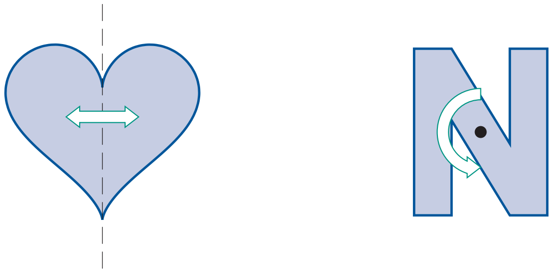


Figure 2 A heart shape and a capital N

Both types of symmetry, reflectional and rotational, are described in terms of transformations that leave a shape as a whole looking the same, namely reflections and rotations. These types of transformations can be used to describe symmetry because they transform shapes *rigidly* – that is, without distorting their size or shape. In other words, they *preserve distances* between points: the distance between any two points is the same as the distance between their images under the transformation. Transformations that have this property are known as *isometries*.

To enable us to formalise these ideas about symmetry, we make the following definitions. You have met the first definition below already, in Unit A1 *Sets, functions and vectors*.

Definitions

A **plane figure** is any subset of the plane $\mathbb{R}^2$.

A **bounded** plane figure is one that can be surrounded by a circle (of finite radius).

For example, the heart shape and the capital N in Figure 2 are bounded plane figures. An infinitely long straight line is a plane figure, but not a bounded plane figure. In the group theory books of this module, we will mainly consider plane figures that are bounded.

We define a *symmetry* of a plane figure as an isometry that maps the figure to itself, as follows, and as illustrated in Figure 3.

Definitions

An **isometry** of the plane is a function $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ that preserves distances; that is, for all points $X, Y \in \mathbb{R}^2$, the distance between $f(X)$ and $f(Y)$ is the same as the distance between X and Y.

A **symmetry** of a plane figure F is an isometry that maps F to itself, that is, an isometry $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ such that $f(F) = F$.

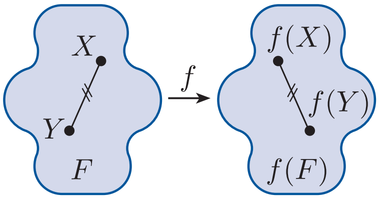


Figure 3 An isometry f preserves distances

As you may have learned in your previous studies, the isometries of the plane are of four types: *rotations*, *reflections*, *translations* and *glide-reflections*. A **rotation** rotates each point of the plane through the same angle about a particular point. A **reflection** reflects each point of the plane in a particular line. A **translation** moves each point of the plane by the same distance in the same direction. A **glide-reflection** is a reflection in a line followed by a translation parallel to that line.

For a *bounded* plane figure, such as the heart shape, any translation (except the translation through zero distance) does not map the figure to itself and so is not a symmetry. The same is true of a glide-reflection (unless the translation involved is the zero translation – in which case the glide-reflection is simply a reflection). So the types of isometries that are potential symmetries of a bounded plane figure are the following.

- The **identity transformation**: equivalent to doing nothing to a figure.
- A **rotation**: specified by a *centre* and an *angle of rotation*, as illustrated in Figure 4(a).
- A **reflection**: specified by a line – an *axis of symmetry*, as illustrated in Figure 4(b).

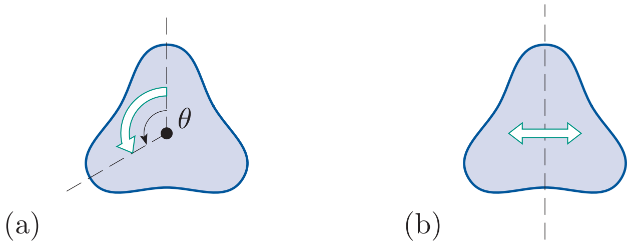


Figure 4 (a) A rotation about a centre through an angle θ (b) A reflection in an axis of symmetry

The identity transformation can be regarded as a zero rotation or a zero translation. We refer to it as the **identity symmetry** of a figure, or just the **identity**. It is sometimes called the **trivial symmetry**.

A **rotational symmetry** is a symmetry that is a rotation, and a **reflectional symmetry** is a symmetry that is a reflection.

When specifying a rotational symmetry, we measure angles anticlockwise, as illustrated in Figure 4(a) (unless otherwise stated), and interpret negative angles as clockwise. The angle $2\pi/3$, for example, specifies an anticlockwise rotation through $2\pi/3$ radians, whereas $-2\pi/3$ specifies a clockwise rotation through $2\pi/3$ radians.

All the rotational symmetries of a *bounded* plane figure have the same centre of rotation (except that the identity symmetry can be regarded as a rotation about any point), and all the axes of symmetry of the figure pass through this centre, as illustrated in Figure 5.

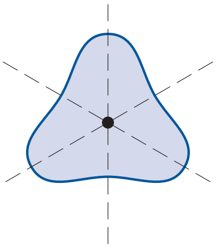


Figure 5 The centre of rotational symmetry and axes of symmetry of a bounded plane figure

Of course, some figures, such as the one in Figure 6, have no symmetries other than the identity symmetry.

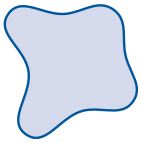


Figure 6 An irregular figure

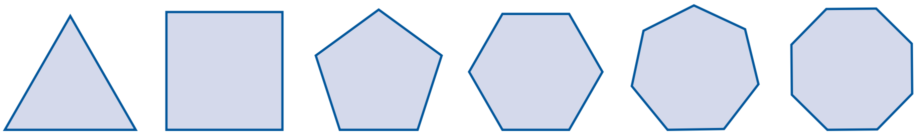
Since a rotation through 2π radians has the same effect on a figure as the identity symmetry, we consider these two transformations to be the same. In general, we have the following definition.

Definition

Two symmetries f and g of a figure F are **equal** if they have the same effect on F, that is, $f(X) = g(X)$ for all points $X \in F$.

The rotation through 0 radians is called the **trivial rotation**; it is equal to the identity symmetry. Any rotation not equal to the trivial rotation is called a **non-trivial rotation**.

We can apply our ideas of symmetry to any plane figure, but we will mainly consider the regular polygons, the first few of which are shown in Figure 7. In general, a **polygon** is a bounded plane figure with straight edges, and a **regular polygon** is a polygon all of whose edges have the same length and all of whose angles are equal.



equilateral triangle — square — regular pentagon — regular hexagon — regular heptagon — regular octagon

Figure 7 Regular polygons

Let us illustrate the ideas by starting with the square. Remember that we consider the square to be a subset of the plane, with its four vertices located at definite positions in $\mathbb{R}^2$. We need a means of tracking the position of the square relative to its initial position after a rotation or a reflection has been carried out.

To do this, imagine a paper model of the square that we can move around in the plane. If we mark a dot in one corner of this paper model, then we can keep track of the position of the square after a rotation. For example, if we take the initial position of the square to be as shown in Figure 8(a), with the dot in the top left corner, then after the square has been rotated anticlockwise through a quarter turn, its position is as shown in Figure 8(b), with the dot in the bottom left corner.

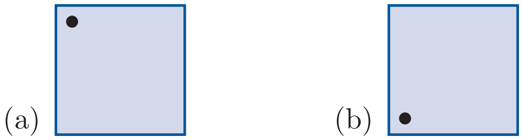


Figure 8 The position of the square (a) initially (b) after it has been rotated through a quarter turn anticlockwise

Using our paper model to keep track of the position of the square after a reflection is not quite so easy. A reflection takes each point of the square to its mirror-image in an axis of symmetry. This is not something we can demonstrate with our paper model by moving it around within the plane.

However, we achieve the same *effect* as a reflection if we 'flip' the paper square along the axis of symmetry. Turning the paper square over in this way takes each point of the square to its mirror-image in the axis of symmetry, just as the reflection does. Therefore, if we colour the two sides of the paper square differently – say, light blue on one side and darker blue on the other – and mark the dot in the same corner on both sides (as if the dot goes through the paper), then we can keep track of the position of the square after a reflection.

For example, if we again take the initial position of the square to be as shown in Figure 9(a), with the dot in the top left corner and the light blue side showing, then after the square has been reflected in the vertical axis of symmetry its position is as shown in Figure 9(b), with the darker side showing and the dot in the top right corner.

Figure 9 The position of the square (a) initially (b) after it has been reflected in the vertical axis of symmetry

We now use this paper model to describe the symmetries of the square. You might find it helpful to make such a model.

The square has four rotational symmetries, namely the rotations about its centre through 0, $\pi/2$, π and $3\pi/2$ radians (anticlockwise), since all of these transformations map the square to itself, as shown in Figure 10. The rotation through 0 radians is just the identity symmetry.

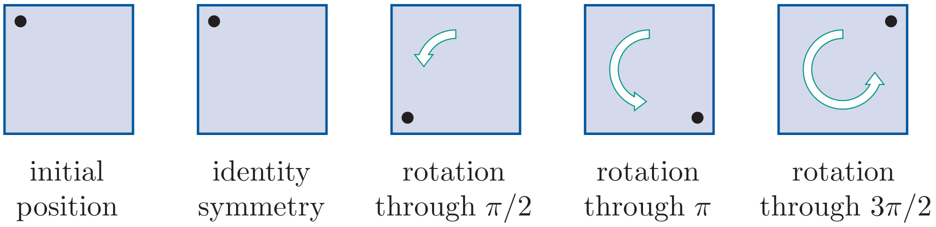


Figure 10 The four rotational symmetries of the square

A rotation through 2π radians returns the square to its original position, and so is the same symmetry as the identity symmetry. Similarly, a rotation through $5\pi/2$ radians is the same symmetry as a rotation through $\pi/2$ radians, because its overall effect on the square is the same. A rotation through $-\pi/2$ radians is the same symmetry as a rotation through $3\pi/2$ radians, because a rotation through $\pi/2$ radians clockwise has the same effect on the square as a rotation through $3\pi/2$ radians anticlockwise.

Now let us consider the reflectional symmetries of the square. The square has four axes of symmetry: a vertical axis, a horizontal axis and two diagonal axes. So it has four reflectional symmetries, as shown in Figure 11.

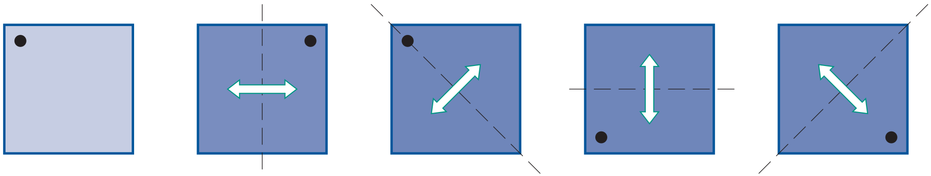


Figure 11 The four reflectional symmetries of the square

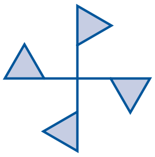
This completes the set of symmetries of the square. It contains eight elements: the identity, three non-trivial rotations and four reflections.

In the next exercise you are asked to find the symmetries of three more plane figures, namely the 4-*windmill* (a symmetric windmill shape with four 'sails'), the rectangle and the equilateral triangle.

Exercise B1

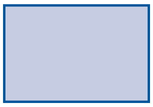
For each of the following figures, describe its set of symmetries by drawing diagrams similar to those given in Figures 10 and 11 for the square.

(a)



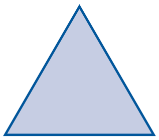
4-windmill

(b)



rectangle

(c)



equilateral triangle

(To hand-draw the light and dark sides of the models reasonably quickly, you could draw them in the way illustrated for the square in Figure 12.)

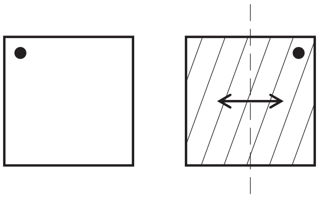


Figure 12 Hand-drawing the paper model of the square

Symmetries of a regular polygon

You saw in Exercise B1(c) that an equilateral triangle has six symmetries: three rotations and three reflections, as shown in Figure 13(a) (recall that we may think of the identity symmetry as a rotation). You have also seen that a square has eight symmetries: four rotations and four reflections, as shown in Figure 13(b).

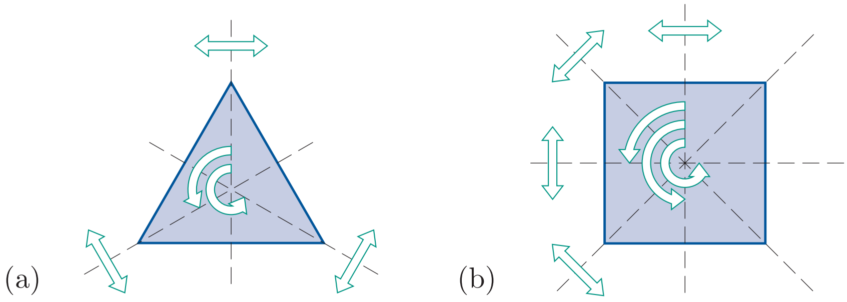


Figure 13 The symmetries of the equilateral triangle and the square (the identity symmetry is not shown)

These are special cases of the following general fact.

A regular polygon with n edges has $2n$ symmetries, namely n rotations (through multiples of $2\pi/n$) and n reflections.

These symmetries are illustrated in Figure 14. A regular polygon with n edges is known as a **regular n-gon**.

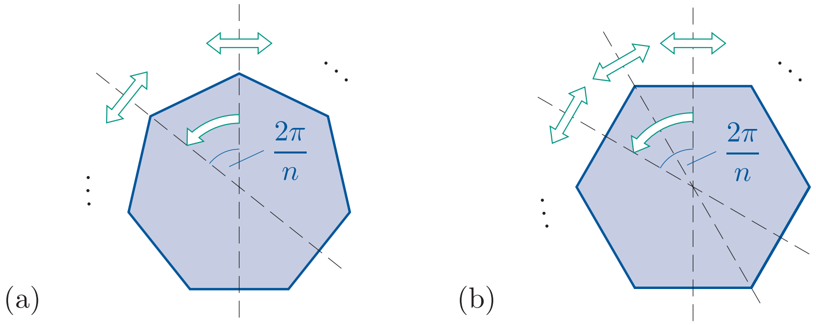


Figure 14 Symmetries of a regular n-gon (a) when n is odd (b) when n is even

For odd values of n, each of the n axes of symmetry passes through a vertex and the midpoint of the opposite edge, as shown in Figure 14(a).

For even values of n, there are $n/2$ axes of symmetry that pass through opposite vertices and $n/2$ axes of symmetry that pass through the midpoints of opposite edges, as shown in Figure 14(b).

1.2 Four properties of the set of symmetries of a plane figure

For any plane figure F, we denote the set of all symmetries of F by $S(F)$. Every figure F has at least one symmetry, namely the identity symmetry, usually denoted by e. So, for every plane figure F, the set $S(F)$ of symmetries of F is non-empty.

In this subsection, you will meet four important properties that the set $S(F)$ always has, no matter what the figure F is.

Closure

Let F be any plane figure. As you saw in the last subsection, the elements of $S(F)$ are the distance-preserving functions $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ such that $f(F) = F$. Suppose that f and g are elements of $S(F)$. Then we can form the composite function $g \circ f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$. (Remember that $\circ$ is read simply as 'circle'.) Since f and g both preserve distance, so must $g \circ f$; and since f and g both map F to itself, so must $g \circ f$, as illustrated in Figure 15. Hence $g \circ f$ is also an element of $S(F)$. So we know that if f and g are elements of $S(F)$, then $g \circ f$ is an element of $S(F)$. We describe this situation by saying that the set $S(F)$ is *closed* under composition of functions. This is our first important property, stated as a proposition in the box below.

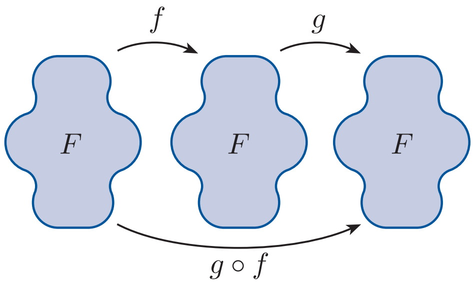


Figure 15 If f and g are symmetries of a plane figure F, then so is $g \circ f$

Proposition B1 Closure property for symmetries

The set of symmetries $S(F)$ of a plane figure F is **closed** under composition of functions; that is, for all elements f and g of $S(F)$, the composite $g \circ f$ is an element of $S(F)$.

So if we take any two symmetries of a plane figure and compose them, then we can recognise the result as a symmetry of the figure.

To illustrate this, let us compose some elements of $S(\square)$, the set of symmetries of the square. (The notation $S(\square)$ is read as 'S square'.)

Figure 16 shows the symmetries of the square, which were described in the previous subsection, and it introduces a labelling for these symmetries that we will use throughout the group theory books of this module. The identity symmetry, which is not shown in Figure 16, is denoted by e, as usual.

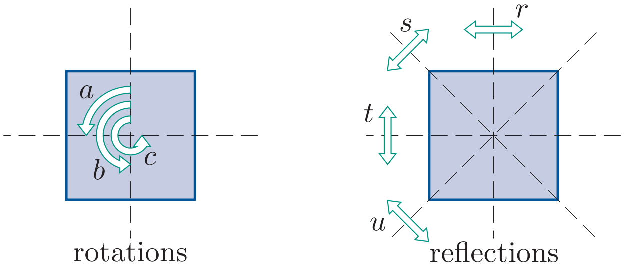


Figure 16 Standard labelling for the elements of $S(\square)$

We will be using the labelling in Figure 16 frequently, so you will probably find it useful to try to remember it. The non-trivial rotations are a, b and c, in order of the angle of rotation, and the reflections are r, s, t and u, starting from the vertical axis of symmetry and working anticlockwise. We will use a similar labelling convention for the symmetries of some of the other regular polygons.

Note that the axes of symmetry of the square are fixed in the plane; so, for example, r means 'reflect in the vertical axis of symmetry, regardless of any symmetries already carried out'. The worked exercise below should clarify what this statement means in practice.

Worked Exercise B1

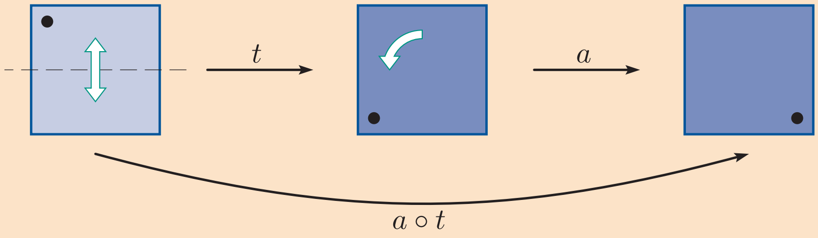
Find the following composites of symmetries of the square.

(a) $a \circ t$ (b) $t \circ a$

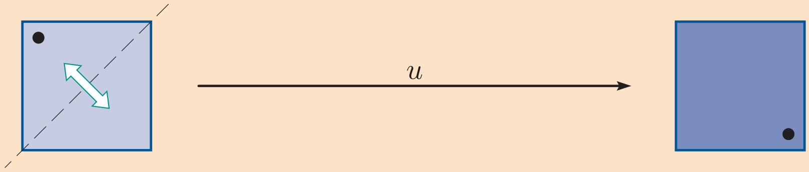
Solution

To keep track of composing the symmetries, we draw pictures of the paper model of the square described earlier, with light and dark sides and a dot in the top left corner. The starting position is always with the light side showing and the dot in the top left corner.

(a) We draw the effect of applying $a \circ t$, that is, first t and then a, to the starting position of the square.



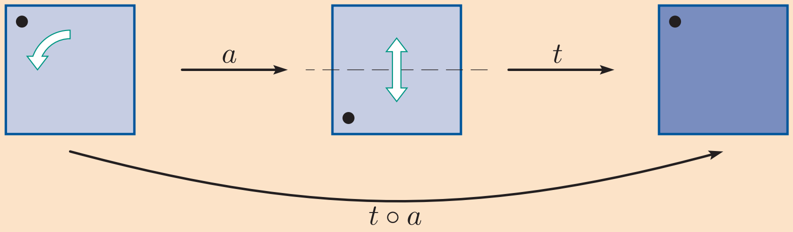
Looking at the final position, we see that the effect of $a \circ t$ is to reflect the square in the diagonal from bottom left to top right, as shown below. This is the same as the effect of the symmetry u.



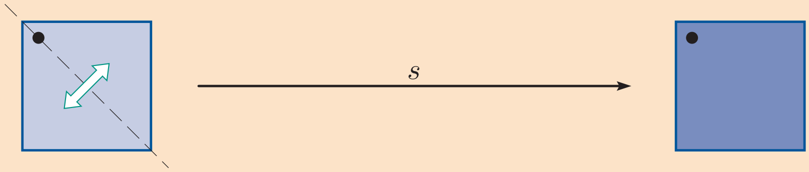
The diagrams show that

$$a \circ t = u.$$

(b) We proceed as in part (a). We draw the effect of $t \circ a$, that is, first a and then t.



We see that the effect of $t \circ a$ is the same as the effect of s.



The diagrams show that

$$t \circ a = s.$$

Notice that in the worked exercise above, $t \circ a \neq a \circ t$.

Here is a similar exercise for you to try.

Exercise B2

Find the following composites of symmetries of the square. (The labelling of the symmetries, introduced in Figure 16, is summarised in Figure 17 for easy reference.)

(a) $b \circ c$ (b) $s \circ s$ (c) $t \circ u$

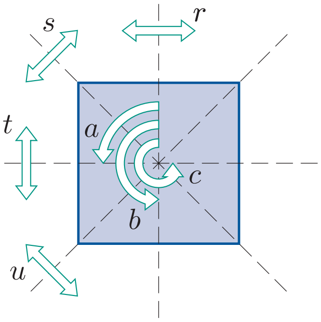


Figure 17 $S(\square)$

Worked Exercise B1 and Exercise B2 illustrate a number of properties of composition of symmetries of a figure F, as follows.

First, order of composition is important. For example, in Worked Exercise B1 you saw that

$$a \circ t = u$$

but

$$t \circ a = s.$$

In general, if $f, g \in S(F)$, then $g \circ f$ may or may not be equal to $f \circ g$. That is, in general, composition of symmetries is not *commutative*.

Second, composition of rotational and reflectional symmetries of a bounded plane figure follows a standard pattern, as follows:

$$\begin{aligned}&\text{rotation} \circ \text{rotation} = \text{rotation},\\ &\text{rotation} \circ \text{reflection} = \text{reflection},\\ &\text{reflection} \circ \text{rotation} = \text{reflection},\\ &\text{reflection} \circ \text{reflection} = \text{rotation}.\end{aligned}$$

For example, in $S(\square)$,

$$b \circ c = a, \quad a \circ t = u, \quad t \circ a = s, \quad t \circ u = c.$$

The pattern above is summarised in the following table:

$\circ$	rotation	reflection
rotation	rotation	reflection
reflection	reflection	rotation

Finally, composing a reflection with itself gives the identity symmetry e.

For example, in $S(\square)$,

$$r \circ r = e, \quad s \circ s = e, \quad t \circ t = e, \quad u \circ u = e.$$

This should be no surprise! If you reflect twice in the same axis then you get back to where you started.

The next exercise is about composing the symmetries of the three plane figures whose symmetries you were asked to find in Exercise B1, namely the 4-windmill, the rectangle and the equilateral triangle. These three shapes are shown in Figure 18, along with the standard labelling that we will use for their symmetries. In each case the identity symmetry is not shown but is denoted by e, as usual.

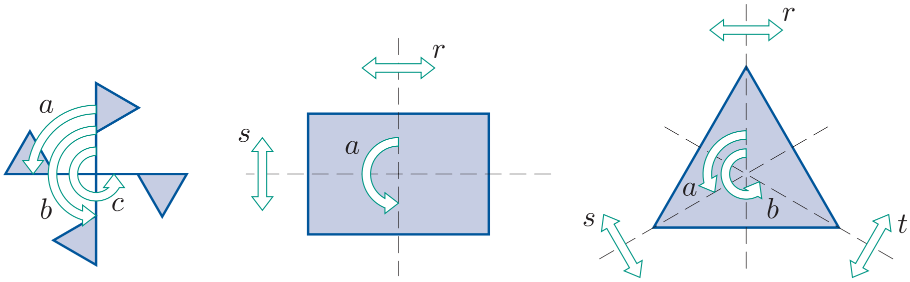


Figure 18 Standard labelling for the elements of $S(✥)$, $S(▭)$ and $S(\triangle)$

Exercise B3

(a) For the 4-windmill, find the following composites of symmetries.

(i) $a \circ b$ (ii) $a \circ c$

(b) For the rectangle, find the following composites of symmetries.

(i) $a \circ r$ (ii) $a \circ s$ (iii) $r \circ s$

(c) For the equilateral triangle, find the following composites of symmetries.

(i) $a \circ b$ (ii) $a \circ r$ (iii) $s \circ t$

Associativity

We now move on to a second important property of the set of symmetries of a figure F. This property is called *associativity*, and it is a general property of composition of functions.

To illustrate it, let us look at an example of composing *three* elements of $S(\square)$, the set of symmetries of the square (see Figure 19). If we want to compose the elements t, a and b, in that order, then we can first compose t with a, and then compose the result with b:

$$b \circ (a \circ t) = b \circ u = s.$$

(Remember that $a \circ t$ means 'do t, then a'. You saw that $a \circ t = u$ in Worked Exercise B1, and you can work out that $b \circ u = s$ using the same method.)

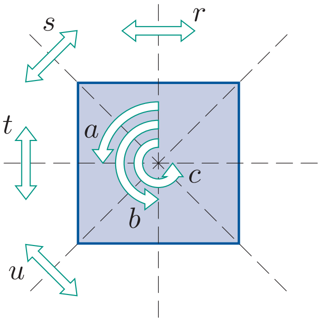


Figure 19 $S(\square)$

Alternatively, we can first compose a with b and then compose t with the result:

$$(b \circ a) \circ t = c \circ t = s.$$

(You can work out that $b \circ a = c$ and $c \circ t = s$ using the method of Worked Exercise B1.)

Notice that we obtain the same answer, s, in each case. This is because essentially both $b \circ (a \circ t)$ and $(b \circ a) \circ t$ mean 'do t, then a, then b'.

In the same way, if F is *any* plane figure, and f, g and h are *any* symmetries in $S(F)$, then

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

We express this fact by saying that composition of symmetries is *associative*. So our second important property is as follows.

Proposition B2 Associativity property for symmetries

Composition of symmetries is associative; that is, if F is a plane figure, then for all $f, g, h \in S(F)$,

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

For practical purposes, associativity means that we do not need to use brackets when we write a composite of three elements: there is no ambiguity in writing simply $h \circ g \circ f$, without brackets, because it does not matter whether we interpret it as $h \circ (g \circ f)$ or $(h \circ g) \circ f$, as both give the same answer.

In fact, associativity tells us that we can write a composite of *any finite number* of elements without brackets; for example we can write $k \circ h \circ g \circ f$, where f, g, h and k are all symmetries of a figure F, without ambiguity. You will see more explanation of this in Subsection 4.1.

Exercise B4

Check that, in $S(\square)$,

$$a \circ (t \circ a) = (a \circ t) \circ a.$$

(In Worked Exercise B1 we found that $a \circ t = u$ and $t \circ a = s$.)

Existence of an identity

At the beginning of this subsection, it was mentioned that any plane figure has at least one symmetry – the identity symmetry. The existence of an identity is our third important property of a set of symmetries. The identity symmetry e has the property that when it is composed with any symmetry $f \in S(F)$, in either order, the result is simply f.

Proposition B3 Identity property for symmetries

The set $S(F)$ of symmetries of a plane figure F contains a special symmetry e (the **identity symmetry**) such that, for each symmetry f in $S(F)$,

$$f \circ e = f = e \circ f.$$

Existence of inverses

We now consider our fourth and final important property of sets of symmetries of plane figures. This property depends on the fact that a symmetry is a one-to-one and onto function from $\mathbb{R}^2$ to $\mathbb{R}^2$. This is because a symmetry, being an isometry, maps $\mathbb{R}^2$ *rigidly* onto itself.

Because a symmetry $f \in S(F)$ is a one-to-one and onto function from $\mathbb{R}^2$ to $\mathbb{R}^2$, it has an inverse function $f^{-1} : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$. Moreover, since f preserves distances and maps F to itself, so must f^{-1}. In other words, f^{-1} is also a symmetry of F, so $f^{-1} \in S(F)$. You saw in Unit A1 that the composite of f and f^{-1}, in either order, is the identity function; that is, it is the identity symmetry e. These conclusions form our fourth important property, stated below.

Proposition B4 Inverses property for symmetries

Each symmetry f in the set $S(F)$ of symmetries of a plane figure F has an **inverse** symmetry f^{-1} in $S(F)$, such that

$$f \circ f^{-1} = e = f^{-1} \circ f.$$

To illustrate this property, let us look again at $S(\square)$.

Worked Exercise B2

Write down the inverse of each of the elements of $S(\square)$.

(The elements of $S(\square)$, except the identity element e, are shown in Figure 20.)

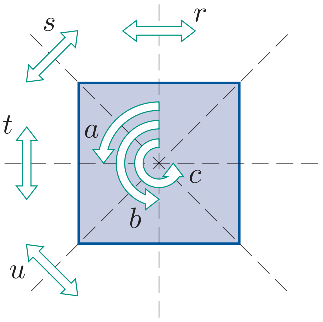


Figure 20 $S(\square)$

Solution

The symmetry a is a rotation through $\pi/2$ about the centre, so its inverse is a rotation through $-\pi/2$ (that is, $\pi/2$ clockwise). This is the same symmetry as c, a rotation through $3\pi/2$.

So c is the inverse of a. Similarly, a is the inverse of c.

The symmetry b is a rotation through a half-turn. Composing b with itself returns the square to its original position. So b is its own inverse.

The symmetries r, s, t and u are all reflections. Composing a reflection with itself returns the square to its original position, so each of these symmetries is its own inverse.

Finally, composing the identity symmetry e with itself returns the square to its original position, so e is also its own inverse.

The inverses of the elements of $S(\square)$ are as follows.

Element	e	a	b	c	r	s	t	u
Inverse	e	c	b	a	r	s	t	u

If a symmetry of a figure is its own inverse, then we say that it is **self-inverse**. Worked Exercise B2 shows that the elements e, b, r, s, t and u of $S(\square)$ are all self-inverse.

Exercise B5

Draw up a table of inverses for each of the following sets of symmetries.

(a) $S($✢$)$ (b) $S(▭)$ (c) $S(\triangle)$

We will return to these four important properties of sets of symmetries of plane figures in Section 3.

1.3 Symmetries of the disc

A bounded figure that we have not yet considered is the disc.Figure 21 shows a rotational symmetry and a reflectional symmetry of the disc.

Figure 21 A rotational symmetry and a reflectional symmetry of the disc

Rotation about the centre through any angle is a symmetry of the disc. Likewise, reflection in any line through the centre is a symmetry of the disc. Thus the disc has infinitely many rotational symmetries and infinitely many reflectional symmetries.

We cannot use individual letters to label these infinitely many symmetries, so we denote a rotation about the centre through an angle θ by r_θ, and a reflection in the axis of symmetry making an angle θ with the horizontal axis by q_θ, as shown in Figure 22.

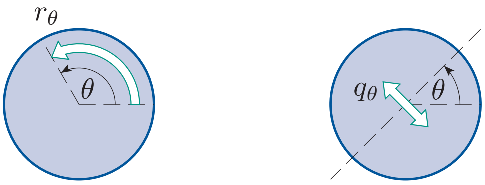


Figure 22 Standard labelling for rotational and reflectional symmetries of the disc

For any integer k, rotations through θ and $\theta + 2k\pi$ produce the same effect as each other, as illustrated in Figure 23(a) for $k = 1$, so we can restrict the angles of rotation to the interval $[0, 2\pi)$. Reflection in the line at an angle θ to the horizontal produces the same effect as reflection in the line at an angle $\theta + \pi$ to the horizontal (in fact, it is the same line), as illustrated in Figure 23(b), so we can restrict the angles for axes of symmetry to the interval $[0, \pi)$.

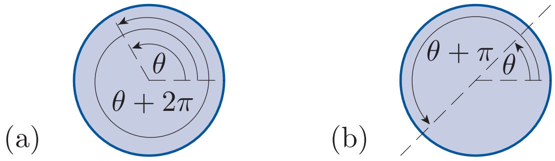


Figure 23 (a) Two angles of rotation that give the same symmetry (b) Two angles that correspond to the same axis of symmetry

So the symmetries of the disc are:

r_θ :	rotation through an angle θ about the centre, for $\theta \in [0, 2\pi)$;
q_θ :	reflection in the line through the centre at an angle θ to the horizontal (measured anticlockwise), for $\theta \in [0, \pi)$.

The identity symmetry e is r_0, the zero rotation. Note that q_0 is reflection in the horizontal axis and is not the identity symmetry.

We denote the set of symmetries of the disc by $S(\bigcirc)$, read as 'S disc':

$$S(\bigcirc) = \{r_\theta : \theta \in [0, 2\pi)\} \cup \{q_\theta : \theta \in [0, \pi)\}.$$

We can compose the symmetries of the disc using diagrams similar to those that we used when composing symmetries of the square. Imagine a paper model of the disc, coloured light blue on one side and a darker blue on the other, with a dot marked at the same place on both sides, as if the dot goes through the paper. We will take the initial position of the disc to be with the light side showing and the dot at the right.

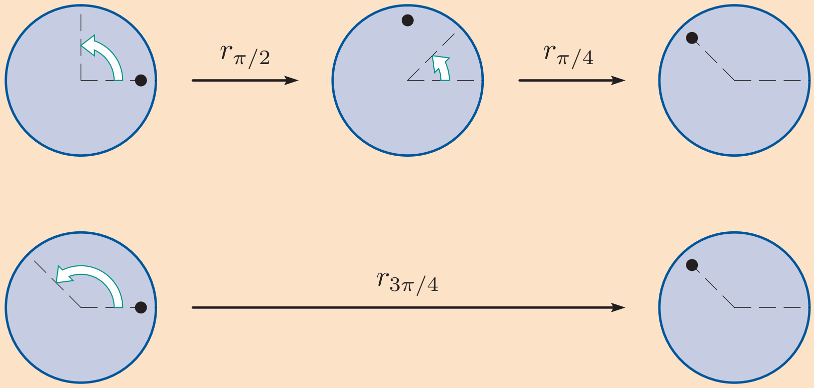
Worked Exercise B3

Find the following composites of symmetries of the disc.

(a) $r_{\pi/4} \circ r_{\pi/2}$ (b) $q_{\pi/4} \circ q_{\pi/2}$ (c) $q_{\pi/4} \circ r_{\pi/2}$

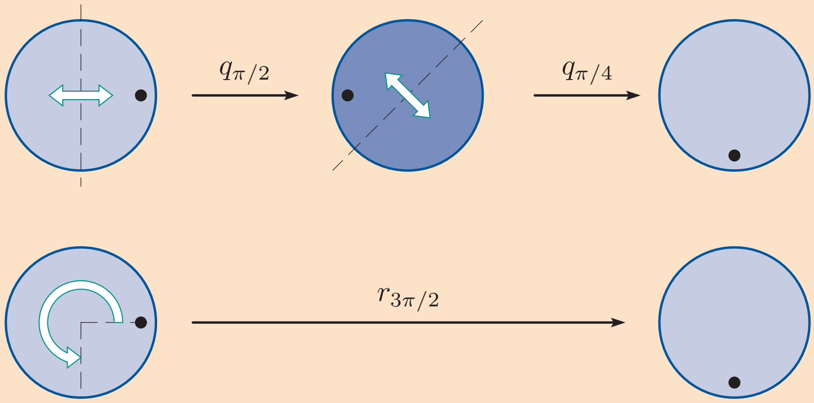
Solution

(a)



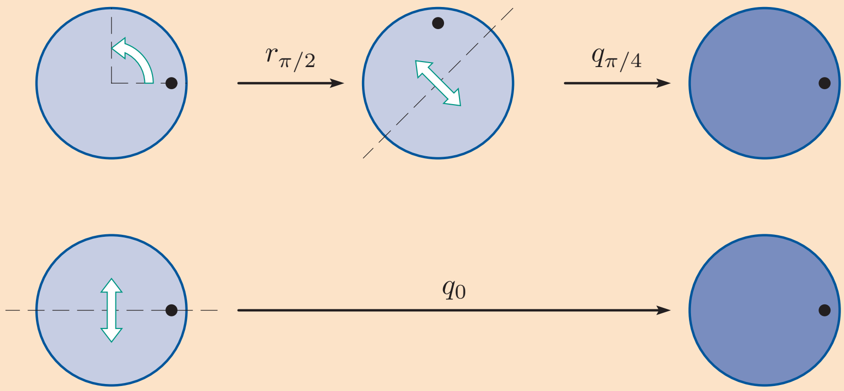
So $r_{\pi/4} \circ r_{\pi/2} = r_{3\pi/4}$.

(b)



So $q_{\pi/4} \circ q_{\pi/2} = r_{3\pi/2}$.

(c)



So $q_{\pi/4} \circ r_{\pi/2} = q_0$.

Exercise B6

Find the composite $r_{\pi/4} \circ q_{\pi/2}$.

There are concise formulas for composing any two symmetries of the disc without having to draw diagrams, but we will not need these formulas in this module.

1.4 Direct and indirect symmetries

In most of the sets of symmetries of plane figures that we have considered, the symmetries are of two sorts: those that we can demonstrate with a paper model without turning it over, and those for which we need to take the model out of the plane, turn it over and replace it in the plane. If we use a paper model that is light on one side and dark on the other, and the initial position is with the light side showing, then the symmetries of the former type are those that result in a final position with the light side showing, and the symmetries of the latter type are those that result in a final position with the dark side showing. We make the following definitions.

Definitions

The symmetries of a plane figure F that we can demonstrate with a paper model without lifting it out of the plane to turn it over are called **direct** symmetries. We denote the set of direct symmetries of a figure F by $S^+(F)$.

The remaining symmetries are called **indirect** symmetries: they are the symmetries that cannot be demonstrated with the paper model without lifting it out of the plane, turning it over and then replacing it in the plane.

For a *bounded* plane figure, the direct symmetries are rotations and the indirect symmetries are reflections. For example, the direct symmetries of the square are the rotations e, a, b and c, so

$$S^+(\square) = \{e, a, b, c\}.$$

The indirect symmetries of the square are the reflections r, s, t and u.

In general, consider any plane figure F that has a finite number of symmetries, and think of our usual type of paper model of F, light on one side and dark on the other. Take the starting position to be a position with the light side showing. Let the number of direct symmetries of F be n. In other words, there are n different ways to pick up the paper model of the figure and place it back down to occupy the same region, with the light side showing. If the figure F has *no* indirect symmetries, then these n direct symmetries are the *only* symmetries of F.

Now suppose that F has at least one indirect symmetry. In other words, it is possible to pick up the paper model of F, turn it over and place it back down to occupy the same region, but with the dark side showing. Once you have done that, there must be n different ways in which you can pick up the paper model again and place it back down to occupy the same region, with the dark side still showing. In other words, F has n indirect symmetries, and if you choose any one of them, then you can obtain all n of them by composing the one that you chose with each of the n direct symmetries in turn.

Figure 24 illustrates this for the square. It shows that each of the four reflections of the square can be obtained by turning the model over and then rotating it.

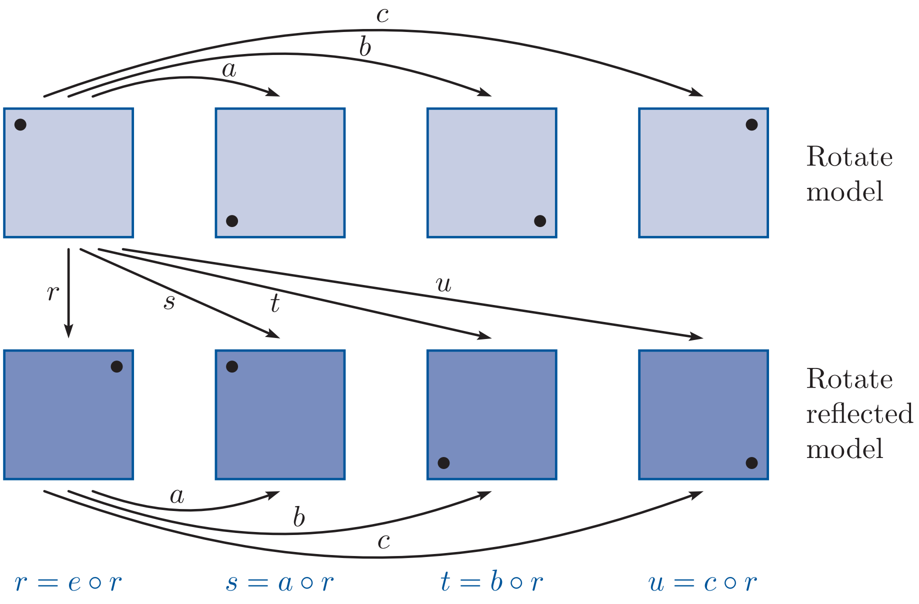


Figure 24 The direct and indirect symmetries of the square

So we have the following useful result.

Theorem B5

If a plane figure has a finite number of symmetries, then either

- all the symmetries are direct, or
- half of the symmetries are direct and half are indirect.

For example, the 4-windmill has only direct symmetries, whereas for the square half of the symmetries are direct and half are indirect.

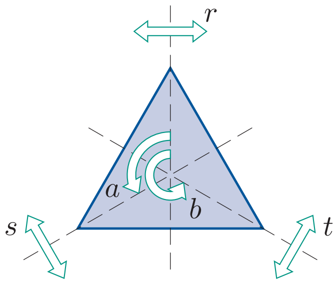


Figure 25 $S(\triangle)$

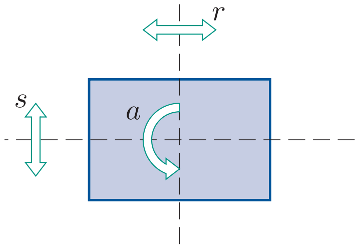


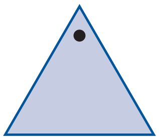
Figure 26 $S(\square)$

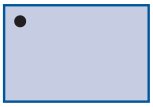
Exercise B7

(a) List the elements of the set of direct symmetries of the equilateral triangle, and draw a diagram (similar to Figure 24) to show how the indirect symmetries of the equilateral triangle can be obtained from the direct symmetries by using just one indirect symmetry.

Use the standard labelling for the elements of $S(\triangle)$, shown in Figure 25, and take the initial position of the triangle to be with the light side showing and the dot in the top corner, as shown below.

(b) Repeat part (a) for the rectangle. Use the standard labelling for the elements of $S(\square)$, shown in Figure 26, and take the initial position to be as shown below.





In Subsection 1.2 you saw some results about composites of rotations and reflections. These can be generalised to corresponding results about direct and indirect symmetries, as follows:

$$\begin{aligned}\text{direct} \circ \text{direct} &= \text{direct},\\ \text{direct} \circ \text{indirect} &= \text{indirect},\\ \text{indirect} \circ \text{direct} &= \text{indirect},\\ \text{indirect} \circ \text{indirect} &= \text{direct}.\end{aligned}$$

∘	direct	indirect
direct	direct	indirect
indirect	indirect	direct

Notice also that the inverse of a direct symmetry is a direct symmetry, and the inverse of an indirect symmetry is an indirect symmetry. This is because for any symmetry f the composite $f \circ f^{-1}$ is equal to the direct symmetry e, so f and f^{-1} are either both direct or both indirect, by the results about composites above.

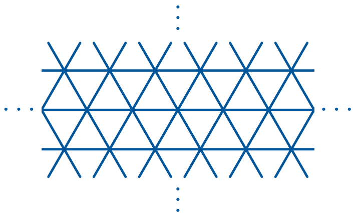


Figure 27 An infinite triangular grid

You have seen in this section that for a *bounded* plane figure the direct symmetries are rotations, and the indirect symmetries are reflections. For an *unbounded* plane figure, such as the infinite triangular grid in Figure 27, the direct symmetries are either rotations or translations, and the indirect symmetries are either reflections or glide-reflections. We will not need to consider translations and glide-reflections further in the group theory books of this module, as we will generally be working with bounded figures.

2 Representing symmetries

So far we have represented symmetries of plane figures by letters, and used diagrams or models to work out composites. This method is illuminating but time-consuming. In this section you will learn a notation for symmetries that allows us to compose them easily, though at the expense of geometric intuition.

2.1 Two-line symbols

To introduce this new notation for symmetries, let us again consider the symmetries of the square. In Figure 28 the locations of the vertices of the square have been labelled with the numbers 1, 2, 3 and 4. We consider these numbers to be fixed to the background plane. So the number 1 is always at the top left-hand corner of the square. It does not label the vertex of the square, and so it does not move when we apply a symmetry to the square.

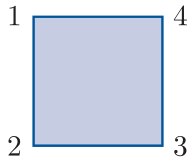


Figure 28 The square with its vertex locations labelled

Here is how we use these numbers to record the effect of a symmetry. Consider, for example, the symmetry a (rotation through $\pi/2$ about the centre), whose effect is shown in Figure 29.

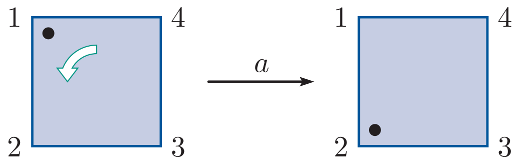


Figure 29 The effect of the symmetry a

This symmetry maps the vertices as follows.

	Shorthand
vertex at location 1 to location 2	$1 \longmapsto 2$
vertex at location 2 to location 3	$2 \longmapsto 3$
vertex at location 3 to location 4	$3 \longmapsto 4$
vertex at location 4 to location 1	$4 \longmapsto 1$

We can think of a as a function mapping the set $\{1,2,3,4\}$ to itself:

$$a:\begin{cases} 1 \longmapsto 2 \\ 2 \longmapsto 3 \\ 3 \longmapsto 4 \\ 4 \longmapsto 1 \end{cases} \quad \text{which we might write as} \quad a:\begin{array}{cccc} 1 & 2 & 3 & 4 \\ \downarrow & \downarrow & \downarrow & \downarrow \\ 2 & 3 & 4 & 1 \end{array}.$$

Our new notation for a is based on the version on the right above, with the arrows omitted and the numbers enclosed in brackets. We write

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Remember that, strictly, the symmetries of the square do not act on the numbers 1, 2, 3, 4. In our new notation we are using these numbers as shorthand for 'the vertex of the square at location 1', 'the vertex of the square at location 2', and so on.

As another example, consider the symmetry r of the square (reflection in the vertical axis), whose effect is shown in Figure 30.

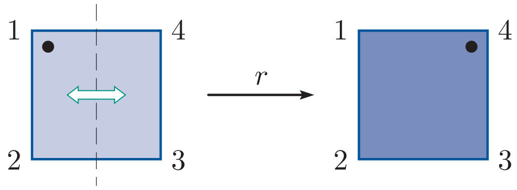


Figure 30 The effect of the symmetry r

This symmetry

interchanges the vertices at locations 1 and 4,

interchanges the vertices at locations 2 and 3.

So, in our new notation, we write

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

The identity symmetry e leaves all the vertices at their original locations, so we write

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

We refer to this new notation for a symmetry of a plane figure as the **two-line symbol** for the symmetry. To specify a symmetry in this form, we must first provide a picture of the figure with labelled locations.

Worked Exercise B4

For the square with vertex locations labelled as shown in Figure 28 (also shown in Figure 31 for convenience), describe geometrically the symmetry represented by the two-line symbol

$$\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 1 & 4 & 3\end{pmatrix}.$$

Identify it as one of the symmetries a, b, c, r, s, t, u of the square (shown in Figure 31).

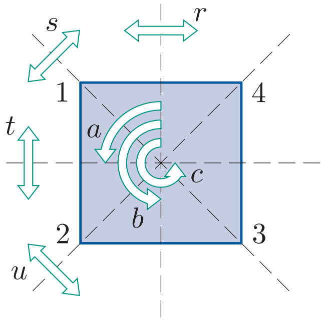


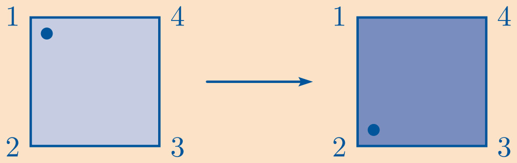
Figure 31 $S(\square)$

Solution

This two-line symbol represents a symmetry that

interchanges the vertices at locations 1 and 2,

interchanges the vertices at locations 3 and 4.



The two-line symbol represents reflection in the horizontal axis. That is, it is the symmetry t.

Exercise B8

Find the two-line symbols representing the symmetries of the square that we have not yet considered, namely b, c, s and u, using the labelling of locations given in Figure 28 (also shown in Figure 31).

Exercise B9

Find the two-line symbol representing each of the four symmetries of the labelled rectangle in Figure 32. (Note that the locations of the vertices are labelled differently from those of the labelled square in Figure 31.)

The two-line symbols that represent the symmetries of a plane figure depend on the choice of labels for locations. For example, you have seen that reflection in the vertical axis is represented by different two-line symbols for the labelled square in Figure 31 and for the labelled rectangle in Figure 32, because we have used different systems for labelling the locations of the vertices (anticlockwise around the square, but across the top and bottom of the rectangle).

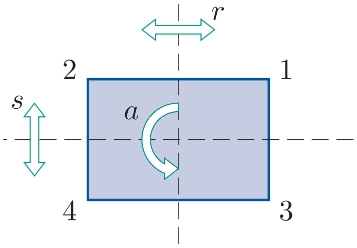


Figure 32 S(▭)

Usually, we try to use an anticlockwise labelling of the locations of the vertices, starting at the top left, as illustrated for the square in Figure 33.

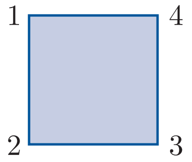


Figure 33 Our usual labelling for the vertex locations of the square

The box below gives a formal definition of a two-line symbol representing a symmetry of a polygon.

Definitions

Let f be a symmetry of a polygon F that has vertices at locations labelled $1, 2, 3, \dots, n$. The **two-line symbol** representing f is

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ f(1) & f(2) & f(3) & \dots & f(n) \end{pmatrix}.$$

where $f(1), f(2), f(3), \dots, f(n)$ are the labels of the locations to which f moves the vertices originally at the locations labelled $1, 2, 3, \dots, n$, respectively.

We say that f is written in **two-line notation**.

The order of the columns in a two-line symbol is not important, though we usually use the natural order to aid recognition. For example, we usually write the two-line symbol

$$\begin{pmatrix} 2 & 4 & 3 & 1 \\ 3 & 1 & 4 & 2 \end{pmatrix} \quad \text{as} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Note that not all possible two-line symbols represent symmetries of a particular figure. For example, with our usual choice of labels for the vertex locations of the square, as shown in Figure 33, the two-line symbol

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix}$$

is not a symmetry of the square, because there is no symmetry of the square that interchanges the vertices at locations 2 and 3, and leaves the vertices at locations 1 and 4 fixed.

With our usual location labels, as shown in Figure 34, the two-line symbols for the eight symmetries of the square are as follows.

$$\begin{array}{ll}
\text{Rotations} & \text{Reflections} \\
e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} & r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \\
a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} & s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} \\
b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} & t = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\
c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} & u = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}
\end{array}$$

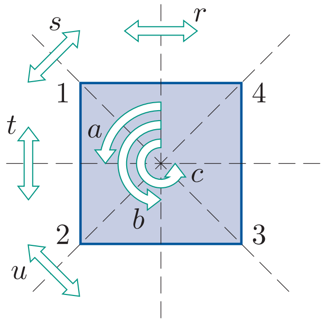


Figure 34 $S(\square)$

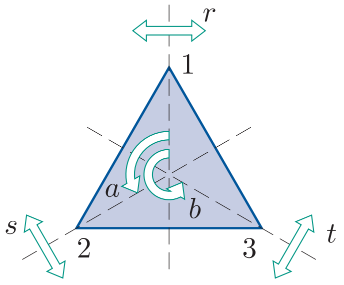


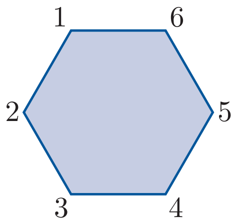
Figure 35 $S(\triangle)$

Exercise B10

Using the labelling in Figure 35 for the locations of the vertices, write down the two-line symbol for each of the symmetries of the equilateral triangle.

Exercise B11

The following two-line symbols represent symmetries of the labelled hexagon shown below. Describe each symmetry geometrically.



(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}$

2.2 Composing and inverting symmetries in two-line notation

One advantage of the two-line notation for symmetries is that it makes it easy to find composites and inverses, without drawing diagrams.

Let us start by looking at composites. In the next worked exercise, we use two-line notation to find the composite of two symmetries of the square.

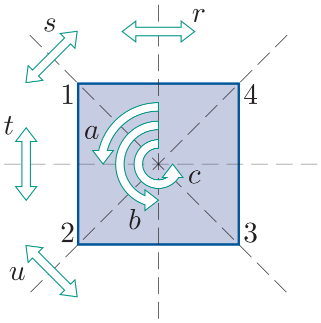


Figure 36 $S(\square)$

The symmetries and standard vertex location labels for the square are repeated in Figure 36 for convenience.

Worked Exercise B5

Use two-line symbols to find the composite $r \circ a$ in $S(\square)$.

Solution

Write down the two-line symbols for r and a (which we found in Subsection 2.1), along with the top row of the two-line symbol for $r \circ a$. Remember that $r \circ a$ means we perform a first, then r.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ & & & \end{pmatrix}.$$

Find each of the entries in the bottom row of $r \circ a$ in turn. First, a sends 1 to 2 and r sends 2 to 3, so $r \circ a$ sends 1 to 3.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & & & \end{pmatrix}.$$

Next, a sends 2 to 3 and r sends 3 to 2, so the composite sends 2 to 2.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & & \end{pmatrix}.$$

Find the final two entries in the same way: a sends 3 to 4 and r sends 4 to 1, so $r \circ a$ sends 3 to 1; and a sends 4 to 1 and r sends 1 to 4, so $r \circ a$ sends 4 to 4.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

We see that $r \circ a$ interchanges the vertices at locations 1 and 3, and keeps the vertices at 2 and 4 where they are. Thus $r \circ a$ is the reflection u.

$$r \circ a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} = u.$$

Remember that the order of composition of symmetries is important. For example,

$$a \circ r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix} = s,$$

so

$$r \circ a \neq a \circ r.$$

Exercise B12

Using the two-line symbols for the symmetries of the equilateral triangle (you were asked to find these in Exercise B10), find the following composites:

$$a \circ a, \quad b \circ s, \quad s \circ b, \quad t \circ s.$$

(The symmetries and standard vertex location labels are shown in Figure 37 for convenience.)

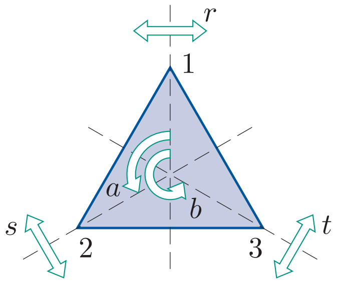


Figure 37 $S(\triangle)$

Now let us look at finding the inverses of symmetries in two-line notation. You saw in Section 1 that every symmetry has an inverse, which 'undoes' the effect of the symmetry.

The worked exercise below demonstrates the method for finding the inverse of a symmetry given as a two-line symbol.

Worked Exercise B6

Find the inverse of the symmetry a in $S(\square)$.

Solution

Find the two-line symbol for a.

We have

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Remember that the inverse a^{-1} 'undoes' the effect of a. So, since a sends 1 to 2, a^{-1} must send 2 to 1; since a sends 2 to 3, a^{-1} must send 3 to 2; and so on. Thus to find a^{-1}, we just have to turn the two-line symbol for a 'upside down'.

So

$$a^{-1} = \begin{pmatrix} 2 & 3 & 4 & 1 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Usually, we then rearrange the columns into the natural order, to make the inverse easier to recognise.

$$= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$$

$$= c.$$

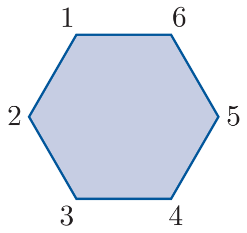


Figure 38 The hexagon, with vertex locations labelled

Exercise B13

Find the inverse of each of the following symmetries of the labelled regular hexagon shown in Figure 38. Give your answers as two-line symbols.

(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$ (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$

2.3 Cayley tables

A useful way to record composites of symmetries is to use a **Cayley table**. To construct a Cayley table for the symmetries of a figure F, we list the elements of $S(F)$ across the top and down the left-hand side of a square array, as illustrated below.

$$\begin{array}{c|ccccccc} & e & f & g & \cdots & x & y & z \\ \hline e & & & & & & & \\ f & & & & & & & \\ g & & & & & & & \\ \vdots & & & & & & & \\ x & & & & & & & \\ y & & & & & & & \\ z & & & & & & & \end{array}$$

The order in which we list the elements is not important, but it is important to use the *same order* across the top and down the side. Normally we put the identity symmetry e first, as shown above.

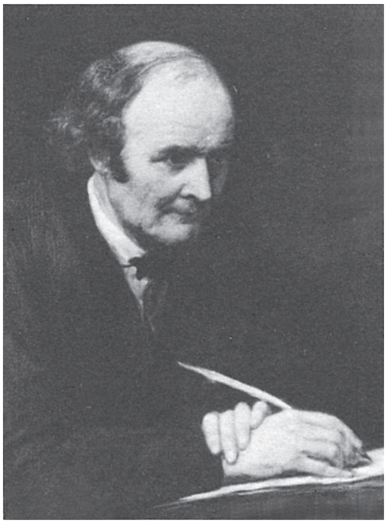
This square array enables us to display every possible composite of pairs of elements in $S(F)$. However, this is practicable only if $S(F)$ is a small set, and it is not possible for $S(\bigcirc)$, which is infinite!

For any two elements x and y of $S(F)$, we record the composite $x \circ y$ in the cell in the row labelled x and the column labelled y.

$$\begin{array}{c|ccc} & \cdots & y & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & x \circ y & \cdots \\ \vdots & & \vdots & \end{array}$$

Note that x is on the left both in the composite and in the border of the table. Of course, the composite $x \circ y$ is the result of performing first the symmetry y and then the symmetry x.

Arthur Cayley (1821–1895) was the leading British algebraist of the nineteenth century. He helped to lay the groundwork for the abstract theory of groups, and he developed the algebra of matrices and determinants. Prior to his appointment in 1863 as the first professor of pure mathematics at the University of Cambridge, he spent fourteen years as a lawyer during which time he produced over three hundred mathematical papers.



Arthur Cayley

We have found many composites of elements of $S(\square)$ already; for example, $a \circ t = u$, $t \circ a = s$ and $r \circ a = u$. A complete Cayley table for $S(\square)$ is given below. The elements of $S(\square)$ are shown in Figure 39.

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

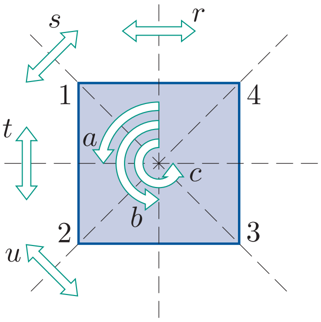


Figure 39 $S(\square)$

Exercise B14

A partially-completed Cayley table for $S(\triangle)$ is shown below. (You were asked to find some of the composites here in Exercise B12, and some others in Exercise B3(c).)

Complete the table, using the two-line symbols from Exercise B10 to work out the required composites. The elements of $S(\triangle)$ are shown in Figure 40.

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e		s	t	
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r		a	b	

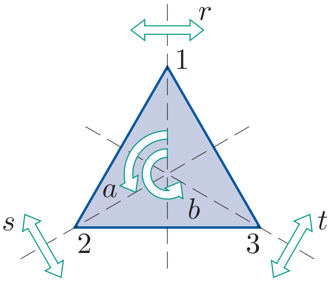


Figure 40 $S(\triangle)$

Exercise B15

Complete the following Cayley table for S(▭). The labelling of the symmetries is as shown in Figure 41.

$\circ$	e	a	r	s
e	e	a	r	s
a	a		s	
r	r	s	e	a
s	s		a	

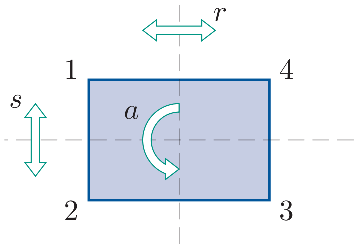


Figure 41 S(▭)

You may have noticed a ‘blocking’ effect in the Cayley table for S(□) above, as highlighted in Figure 42(a), and a similar effect in the Cayley table for S(△) found in Exercise B14. This effect occurs because we have chosen to list all the direct symmetries first in the borders of the table, followed by the indirect symmetries, and, as you saw earlier, a composite of any two direct symmetries or any two indirect symmetries is always a direct symmetry, and a composite of a direct symmetry and an indirect symmetry is always an indirect symmetry. This gives the blocking shown in Figure 42(b).

$\circ$	e	a	b	c	r	s	t	u
e	e	a	b	c	r	s	t	u
a	a	b	c	e	s	t	u	r
b	b	c	e	a	t	u	r	s
c	c	e	a	b	u	r	s	t
r	r	u	t	s	e	c	b	a
s	s	r	u	t	a	e	c	b
t	t	s	r	u	b	a	e	c
u	u	t	s	r	c	b	a	e

(a)

$\circ$	direct	indirect
direct	direct	indirect
indirect	indirect	direct

(b)

Figure 42 ‘Blocking’ into direct and indirect symmetries

A similar blocking effect occurs in the Cayley table for the set of symmetries of any plane figure that has indirect symmetries, when we list all the direct symmetries first in the borders of the table.

3 Definition of a group

You are now ready to learn what is meant by a *group*.

3.1 The group axioms

In Subsection 1.2 you saw that if F is a plane figure, then any two symmetries in the set $S(F)$ of symmetries of F can be composed, and the following four properties hold.

- **Closure** The composite of any two symmetries in $S(F)$ is a symmetry in $S(F)$.
- **Associativity** Composition of symmetries is associative.
- **Identity** The set $S(F)$ contains an identity symmetry.
- **Inverses** Each symmetry f in $S(F)$ has an inverse symmetry.

There are many other circumstances in which we have some set, with a means of combining any two elements of the set, in which four properties analogous to those above hold. For example, consider the set $\mathbb{R}$ of real numbers, with addition as the means of combining any two elements. As you know from Unit A2 *Number systems*, the following four properties hold; compare them to the properties above.

- **Closure** (A1) The sum of any two numbers in $\mathbb{R}$ is a number in $\mathbb{R}$.
- **Associativity** (A2) Addition of numbers in $\mathbb{R}$ is associative (that is, $(x+y)+z = x+(y+z)$ for all $x, y, z \in \mathbb{R}$).
- **Identity** (A3) The set $\mathbb{R}$ contains an identity element (namely 0, since adding 0 to any real number leaves the number unchanged).
- **Inverses** (A4) Every number in $\mathbb{R}$ has an inverse number (the inverse of x is $-x$, because adding x and $-x$ gives the identity element 0).

A means of combining any two elements of a set is called a **binary operation** on the set. For example, function composition is a binary operation on the set of symmetries of a figure, and addition is a binary operation on the set $\mathbb{R}$. Similarly, multiplication is a binary operation on the set $\mathbb{R}$, and addition modulo n and multiplication modulo n are binary operations on the set $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$, for any integer $n \geq 2$.

When we have a set, together with a binary operation on the set, such that four properties analogous to those above hold, we say that the set and the binary operation together form a mathematical structure known as a *group*. So the set of symmetries of a figure with the operation of function composition forms a group, as does the set $\mathbb{R}$ with the operation of addition.

Here is the formal definition of a group. In this definition, G represents a set of any kind of objects, and $\circ$ (which is read, as usual, as 'circle') represents any binary operation defined on G (it does not necessarily represent function composition). The set G may be either finite or infinite.

Definition

Let G be a set and let $\circ$ be a binary operation defined on G. Then $(G, \circ)$ is a **group** if the following four axioms hold.

G1 Closure For all g, h in G,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for $\circ$ on G.)

G4 Inverses For each element g in G, there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to $\circ$.)

We refer to axioms G1–G4 as the **group axioms**. In mathematics, an **axiom** is a mathematical statement that is used as a starting point from which other mathematical statements are deduced.

We often refer to an identity element simply as an **identity**, and to an inverse element of an element g simply as an **inverse** of g. An alternative way to say that $(G, \circ)$ is a group is to say that G is a group **under** $\circ$.

The word *group* was introduced by the French mathematician Évariste Galois (1811–1832), as part of a theory to classify the polynomial equations whose solutions can be expressed by a formula involving *radicals* (nth roots). However, what Galois meant by a group was somewhat different to the modern definition of the term. His memoir on this topic, which was written in 1830, lay unpublished until 1846, several years after his untimely death from wounds received in a duel.

Évariste Galois

Notice that the binary operation $\circ$ of a group need *not* have the property that

$$g \circ h = h \circ g \quad \text{for all } g, h \text{ in } G.$$

That is, the binary operation does not have to be **commutative**. A group that has this additional property is given a special name.

Definitions

A group $(G, \circ)$ that has the additional property that

$$g \circ h = h \circ g \quad \text{for all } g, h \text{ in } G$$

is an **abelian** (or **commutative**) group.

A group that is not abelian is **non-abelian**.

For example, the set of real numbers, with addition, is an abelian group, because addition of real numbers is commutative. On the other hand, the set of symmetries of the square, with function composition, is a non-abelian group, since composing symmetries of the square in different orders can give different results, as you saw in Subsection 1.2.

Abelian groups are named after the Norwegian mathematician Niels Henrik Abel (1802–1829), who in 1824 showed that no formula involving radicals exists for the solutions of a general polynomial equation of degree 5. Formulas for the solutions of general polynomial equations of degrees 3 and 4 had been found in the 16th century, although they were written without the benefit of modern notation.

Since Abel initially had to publish his result at his own expense, he compressed the proof in order to save money, and this made it very hard to understand. It was only later, after he had the opportunity to rewrite an elaborated version for publication in a German journal, that his work became widely known.

Niels Henrik Abel

Here are some more definitions that are useful when we discuss groups.

Definitions

- If the set G of a group $(G, \circ)$ is a finite set, then we say that $(G, \circ)$ is a **finite** group. If G has exactly n elements, then we say that $(G, \circ)$ is a group of **order** n, and we write $|G| = n$.
- If the set G of a group $(G, \circ)$ is an infinite set, then we say that $(G, \circ)$ is an **infinite** group and that it has **infinite order**.

For example, the set $S(\square)$ of symmetries of the square, with function composition, is a finite group and has order 8. We write $|S(\square)| = 8$. The set of real numbers, with addition, is an infinite group.

As you saw in Unit A2 *Number systems*, an identity element for a binary operation on a set is sometimes called an **additive identity** if the binary operation is addition, and a **multiplicative identity** if the binary operation is multiplication. Similarly, an inverse of a particular element is sometimes called an **additive inverse** if the binary operation is addition, and a **multiplicative inverse** if the binary operation is multiplication.

In Unit A2 you saw that a *field* is a set with two operations, $+$ and $\times$, such that twelve properties hold. These twelve properties are called the *field axioms*, though we did not use that term in Unit A2. A field can be defined more concisely in terms of groups, as follows. If F is a set, and $+$ and $\times$ are binary operations defined on F, then we say that $(F, +, \times)$ is a **field** if it has the following three properties.

- $(F, +)$ is an abelian group.
- $(F - \{0\}, \times)$ is an abelian group (where 0 is the identity element for $+$ on F).
- The distributive law $x \times (y + z) = (x \times y) + (x \times z)$ holds for all $x, y, z \in F$.

3.2 Checking the group axioms

To show that a given set and binary operation form a group, we need to check that they satisfy the four group axioms.

The worked exercise below demonstrates how to show formally that the set $\mathbb{R}$ of real numbers, with addition, forms a group.

Worked Exercise B7

Show that $(\mathbb{R}, +)$ is a group.

Solution

We show that the four group axioms hold.

G1 Closure

We have to check that if we add any two elements of $\mathbb{R}$, then we always get another element of $\mathbb{R}$. We can use x and y, say, to denote general elements of $\mathbb{R}$.

For all $x, y \in \mathbb{R}$,

$$x + y \in \mathbb{R}.$$

So $\mathbb{R}$ is closed under addition.

G2 Associativity

We already know that addition of numbers is an associative operation.

Addition of real numbers is associative.

G3 Identity

We have to check that the set $\mathbb{R}$ contains a special element such that, when this element is added to any other element, in either order, the result is simply that other element.

We have $0 \in \mathbb{R}$, and for all $x \in \mathbb{R}$,

$$x + 0 = x = 0 + x.$$

So 0 is an identity element for addition on $\mathbb{R}$.

G4 Inverses

We have to check that for each element x in $\mathbb{R}$, there is an element in $\mathbb{R}$ such that, when this element is added to x, in either order, the result is the identity element 0.

For each $x \in \mathbb{R}$, we have $-x \in \mathbb{R}$, and

$$x + (-x) = 0 = (-x) + x,$$

so $-x$ is an inverse of x.

Thus each element of $\mathbb{R}$ has an inverse element in $\mathbb{R}$ with respect to addition.

Hence $(\mathbb{R}, +)$ satisfies the four group axioms, and so is a group.

There are several things that it is useful to observe about Worked Exercise B7.

First, notice that when you check axioms G3 (identity) and G4 (inverses), you have to check *both possible orders* of combining two elements. For example, when we checked axiom G3 in Worked Exercise B7, we checked not only that $x + 0 = x$, but also that $0 + x = x$. Similarly, when we checked axiom G4, we checked not only that $x + (-x) = 0$, but also that $(-x) + x = 0$. This checking was straightforward in Worked Exercise B7, because the binary operation was addition, and order does not matter when you add two numbers. However, for some binary operations the checking can involve more work.

Second, notice that when we checked axiom G3 (identity) in Worked Exercise B7, it was fairly obvious that the identity element had to be 0. In general, if you are dealing with a set of numbers and the binary operation is ordinary addition, then the only possible identity element is 0. (This is because the only possibility for a number e that satisfies the equation $g + e = g$ for all numbers g is $e = 0$.) Similarly, if you are dealing with a set of numbers and the binary operation is ordinary multiplication, then the only possible identity element is 1. For other binary operations, *including modular addition and modular multiplication*, it may be less obvious what the identity element has to be. You just have to try to find a possibility and check that it works.

A similar point applies to axiom G4 (inverses). If you are dealing with a set of numbers and the binary operation is ordinary addition, then the only possible inverse of an element x is $-x$; if you are dealing with a set of numbers and the binary operation is ordinary multiplication, then the only possible inverse of an element x is $1/x$. For other binary operations it may be less obvious what the inverses have to be.

Third, notice that when you check axiom G3 (identity) it is not enough to check that a particular element *is* an identity element. You also have to check that this element *actually lies in the set* that you are considering. Similarly, when you check axiom G4 (inverses), not only do you have to check that each element *has* an inverse, you also have to check that each inverse *lies in the set* that you are considering.

Finally, notice that when you check axiom G2 (associativity), if the binary operation that you are dealing with is one that you already know is associative, such as the operations in the box below, then you can simply state that it is associative, without proof. We did this in Worked Exercise B7. However, if the binary operation is unfamiliar, then you have to provide a proof of associativity.

Standard associative binary operations

- Addition
- Multiplication
- Function composition
- Modular addition
- Modular multiplication

You might find it helpful to refer back to the comments above as you work through the rest of this subsection. Below is another worked exercise that illustrates some of these points. Here the binary operation is multiplication (rather than addition, as in the previous worked exercise). The set is $\mathbb{R}^*$, that is, the set $\mathbb{R} - \{0\}$ of all the real numbers except 0.

Worked Exercise B8

Show that $(\mathbb{R}^*, \times)$ is a group.

Solution

We show that the four group axioms hold.

G1 Closure

We have to check that if we multiply any two elements of $\mathbb{R}^*$, we always get another element of $\mathbb{R}^*$. To specify that x and y, say, represent *any* elements of $\mathbb{R}^*$, we can say 'Let $x, y \in \mathbb{R}^*$.'

Let $x, y \in \mathbb{R}^*$. Then, since x and y are real numbers, so is $x \times y$.

Also $x \times y \neq 0$, since $x \neq 0$ and $y \neq 0$. Hence

$$x \times y \in \mathbb{R}^*,$$

so $\mathbb{R}^*$ is closed under multiplication.

G2 Associativity

We already know that multiplication of numbers is associative.

Multiplication of real numbers is associative.

G3 Identity

We have to check that the set $\mathbb{R}^*$ contains a special element such that when this element is multiplied by any other element, in either order, the result is simply that other element.

We have $1 \in \mathbb{R}^*$, and for all $x \in \mathbb{R}^*$,

$$x \times 1 = x = 1 \times x.$$

So 1 is an identity element for multiplication on $\mathbb{R}^*$.

G4 Inverses

We have to check that for each element x in $\mathbb{R}^*$, there is an element in $\mathbb{R}^*$ such that when this element is multiplied by x, in either order, the result is the identity element 1.

Let $x \in \mathbb{R}^*$. Then $x \neq 0$, so $1/x$ exists, and lies in $\mathbb{R}^*$, since $1/x \neq 0$. Also

$$x \times \frac{1}{x} = 1 = \frac{1}{x} \times x.$$

Hence $1/x$ is an inverse of x.

Thus each element of $\mathbb{R}^*$ has an inverse element in $\mathbb{R}^*$ with respect to multiplication.

Hence $(\mathbb{R}^*, \times)$ satisfies the four group axioms, and so is a group.

You can practise applying the four group axioms for yourself in the next exercise. The notation $\mathbb{Q}^*$ in part (b) denotes the set $\mathbb{Q} - \{0\}$ of all the rational numbers except 0.

Exercise B16

Show that each of the following is a group.

(a) $(\mathbb{Z}, +)$ (b) $(\mathbb{Q}^*, \times)$

You have seen that to prove that a set G and binary operation $\circ$ form a group, you have to show that all four group axioms hold. It follows that to show that a set and binary operation *do not* form a group, you just need to show that *any one* of the four group axioms fails. Here is an example.

Worked Exercise B9

Show that $(\mathbb{R}, \times)$ is not a group.

Solution

We check each axiom in turn until we find one that fails.

We check the four group axioms.

G1 Closure

If we multiply any two elements of $\mathbb{R}$, do we always get another element of $\mathbb{R}$?

For all $x, y \in \mathbb{R}$,

$$x \times y \in \mathbb{R}.$$

So $\mathbb{R}$ is closed under multiplication.

Axiom G1 holds.

G2 Associativity

Multiplication of real numbers is associative.

Axiom G2 holds.

G3 Identity

Does $\mathbb{R}$ contain a special element such that when this element is multiplied by any other element, in either order, the result is that other element?

We have $1 \in \mathbb{R}$, and for all $x \in \mathbb{R}$,

$$x \times 1 = x = 1 \times x.$$

So 1 is an identity element for × on $\mathbb{R}$ (and the only possibility to be such an identity element).

Axiom G3 holds.

G4 Inverses

For each element x in $\mathbb{R}$, is there is an element in $\mathbb{R}$ such that when this element is multiplied by x, in either order, the result is the identity element 1?

No! For nearly every element x in $\mathbb{R}$, the element $1/x$ has the required property. But there is no element with the required property for 0.

The element 0 is in $\mathbb{R}$, but it has no inverse with respect to multiplication in $\mathbb{R}$. This is because there is no element y, say, in $\mathbb{R}$ that has the property that

$$0 \times y = 1.$$

Hence axiom G4 does not hold.

It follows that $(\mathbb{R}, \times)$ is not a group.

In general, to show that a particular set and binary operation do not form a group, you need to show that one of the group axioms fails, by demonstrating that there is a counterexample to the axiom. For instance, in Worked Exercise B9 we pointed out that, for the set $\mathbb{R}$ and binary operation ×, the number 0 is a counterexample to axiom G4 (inverses).

Although in Worked Exercise B9 we checked all the group axioms in turn until we found one that failed, if you can immediately spot an axiom that fails, then you can go straight to that axiom and provide a counterexample, without working through the preceding axioms. The only exception to this is that if you want to show that axiom G4 (inverses) fails, then, since you need an identity element for axiom G4 to make sense, you have to begin by establishing what this identity element must be. That is, you have first to consider axiom G3 (identity) to some extent.

The next worked exercise gives, for each of the four axioms, an example of how we can show that the axiom in question fails.

Worked Exercise B10

(a) Let D be the set of odd integers. Show that $(D, +)$ is not a group, by showing that axiom G1 (closure) fails.

(b) Show that $(\mathbb{R}, -)$ is not a group, by showing that axiom G2 (associativity) fails.

(c) Let E be the set of even integers. Show that $(E, \times)$ is not a group, by showing that axiom G3 (identity) fails.

(d) Show that $(\mathbb{N}, \times)$ is not a group, by showing that axiom G4 (inverses) fails. (Remember that $\mathbb{N}$ is the set of natural numbers, that is, positive integers.)

Solution

(a) The numbers 3 and 5 lie in D, but

$$3 + 5 = 8 \notin D.$$

So D is not closed under $+$. That is, axiom G1 fails.

(b) Consider the numbers 6, 4 and 1 in $\mathbb{R}$. We have

$$6 - (4 - 1) = 6 - 3 = 3,$$

but

$$(6 - 4) - 1 = 2 - 1 = 1.$$

These expressions are not equal, so this counter-example shows that subtraction is not associative on $\mathbb{R}$. That is, axiom G2 fails.

(c) There is no element $e \in E$ such that

$$2 \times e = 2,$$

because $1 \notin E$. So $(E, \times)$ has no identity element. That is, axiom G3 fails.

(d) The number 1 is the only possible identity element for $(\mathbb{N}, \times)$. However, $2 \in \mathbb{N}$, and there is no number n, say, in $\mathbb{N}$ such that

$$2 \times n = 1,$$

because $\frac{1}{2} \notin \mathbb{N}$. So the element 2 of $\mathbb{N}$ has no inverse in $\mathbb{N}$. Hence axiom G4 fails.

Sometimes, as in the next exercise, you may need to determine whether a particular set and binary operation form a group, rather than being told this from the start and asked to prove it. In this sort of situation, it is worth having a quick think to see whether you can spot an axiom that fails. Often when a set and binary operation do not form a group, more than one of the axioms fails. If you cannot immediately spot an axiom that fails, then usually the best way to proceed is to work through the four axioms systematically, until either you have proved that they all hold, or you have found one that fails.

Exercise B17

For each of the following, either show that the given set and binary operation form a group, or show that they do not.

(a) $(\mathbb{Q}, \times)$

(b) $(\mathbb{R}^+, +)$, where $\mathbb{R}^+$ is the set of positive real numbers.

(c) $(D, \times)$, where D is the set of odd integers.

(d) $(E, +)$, where E is the set of even integers.

(e) $(E, -)$, where E is the set of even integers.

(f) $(M, \times)$, where M is the set whose elements are all the negative real numbers and the number 1; that is, $M = \{x \in \mathbb{R} : x < 0\} \cup \{1\}$.

Unfamiliar binary operations

In all the examples that you have seen so far, the binary operation has been a familiar one, such as addition, multiplication or function composition. In the next worked exercise, the binary operation is unfamiliar.

Worked Exercise B11

Determine whether $(\mathbb{R}, \circ)$ is a group, where $\circ$ is defined by

$$x \circ y = x + y + xy.$$

Solution

We check the four group axioms.

G1 Closure

For all $x, y \in \mathbb{R}$,

$$x \circ y = x + y + xy \in \mathbb{R},$$

since sums and products of real numbers are real numbers. So $\mathbb{R}$ is closed under $\circ$.

G2 Associativity

For each $x, y, z \in \mathbb{R}$, we have

$$\begin{aligned} x \circ (y \circ z) &= x \circ (y + z + yz) \\ &= x + (y + z + yz) + x(y + z + yz) \\ &= x + y + z + yz + xy + xz + xyz \\ &= x + y + z + xy + xz + yz + xyz \end{aligned}$$

and

$$\begin{aligned}(x \circ y) \circ z &= (x + y + xy) \circ z \\ &= (x + y + xy) + z + (x + y + xy)z \\ &= x + y + xy + z + xz + yz + xyz \\ &= x + y + z + xy + xz + yz + xyz.\end{aligned}$$

The two expressions obtained are the same, so $\circ$ is associative on $\mathbb{R}$.

G3 Identity

Try to find a likely candidate to be an identity element.

We need an element $e \in \mathbb{R}$ such that, for all $x \in \mathbb{R}$,

$$x \circ e = x = e \circ x.$$

The left-hand equation $x \circ e = x$ gives

$$x + e + xe = x,$$

which simplifies to

$$e(1 + x) = 0.$$

Since we need this equation to be true for all $x \in \mathbb{R}$, the only possibility for an identity element is $e = 0$.

Now check to see whether 0 actually is an identity element.

Now $0 \in \mathbb{R}$, and for all $x \in \mathbb{R}$,

$$x \circ 0 = x + 0 + x0 = x,$$

and

$$0 \circ x = 0 + x + 0x = x,$$

as required. So 0 is an identity element for $\circ$ on $\mathbb{R}$.

G4 Inverses

Try to find a likely candidate to be an inverse of a general element x.

For each $x \in \mathbb{R}$, we need an element y, say, in $\mathbb{R}$ such that

$$x \circ y = 0 = y \circ x.$$

The left-hand equation $x \circ y = 0$ gives

$$x + y + xy = 0.$$

Try to solve this equation for y.

This equation can be rearranged as

$$y(1 + x) = -x,$$

so, for $x \neq -1$,

$$y = -\frac{x}{1+x},$$

and this element is in $\mathbb{R}$.

So it looks like every element x in $\mathbb{R}$ except possibly -1 has an inverse, given by $-x/(1+x)$. But what about -1: does it have an inverse?

If the element -1 has an inverse y, then

$$(-1) \circ y = 0 = y \circ (-1).$$

The left-hand equation $(-1) \circ y = 0$ gives

$$-1 + y - y = 0,$$

which simplifies to

$$-1 = 0.$$

This conclusion is false, so -1 has no inverse.

Hence axiom G4 fails, and therefore $(\mathbb{R}, \circ)$ is not a group.

In the worked exercise above, you saw that the set $\mathbb{R}$ is not a group under the binary operation $\circ$ given by $x \circ y = x + y + xy$, because the element -1 has no inverse and so axiom G4 fails. In fact, if you remove the element -1 from $\mathbb{R}$ then you *do* obtain a group under this binary operation. There is a 'challenging' exercise in the additional exercises booklet for this unit that asks you to prove this.

You can practise working with unfamiliar binary operations in the exercises below.

Exercise B18

Show that $(\mathbb{R}, \circ)$, where $\circ$ is defined by

$$x \circ y = x - y - 1,$$

is not a group, by showing that group axiom G3 (identity) fails.

Exercise B19

Determine whether each of the following binary operations $\circ$ defined on $\mathbb{R}$ is associative.

(a) $x \circ y = x + y - xy$ (b) $x \circ y = x - y + xy$

Exercise B20

Show that $(\mathbb{Q}^+, \circ)$ is a group, where $\mathbb{Q}^+$ is the set of positive rational numbers and $\circ$ is defined by $a \circ b = \frac{1}{2}ab$.

3.3 Checking the group axioms for small finite sets

In the previous subsection you saw how to check the group axioms for a variety of sets and binary operations. In all the examples, the set was an infinite set. In this subsection we concentrate on how to check the group axioms when the set is a small finite set.

Most of the examples of small finite sets and binary operations that we will consider in this subsection come from modular arithmetic, which you met in Unit A2. Remember that for any natural number n we have

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\},$$

and the operations $+_n$ and $\times_n$ on $\mathbb{Z}_n$ are defined by

$$a +_n b = \text{the remainder of } a + b \text{ on division by } n,$$
$$a \times_n b = \text{the remainder of } a \times b \text{ on division by } n.$$

For example, $\mathbb{Z}_4 = \{0, 1, 2, 3\}$, and we have

$$2 +_4 3 = 1,$$
$$2 \times_4 3 = 2.$$

If we have a small finite set with a binary operation (where the set and binary operation come from modular arithmetic or from anywhere else), then we can construct a Cayley table for them, in the same way as we did for sets of symmetries earlier. As you will see in this subsection, we can use this table to help us check some of the group axioms.

To construct a Cayley table for a small finite set G and binary operation $\circ$, we use the same approach as for a set of symmetries. We list the elements of G across the top and down the side of a square array, keeping the order of the elements the same across the top and down the side. If we can immediately spot an identity element, then usually we put it first in the list, but this is not essential.

For any two elements x and y of G, we enter the composite $x \circ y$ in the cell in the row labelled x and the column labelled y, as shown below. So x is on the left both in the composite and in the row labels down the left of the table.

$$\begin{array}{c|ccc} \circ & \cdots & y & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & x \circ y & \cdots \\ \vdots & & \vdots & \end{array}$$

We refer to the lists of elements along the top and down the side of a Cayley table as the **borders** of the table, and we refer to the rest of the table as its **body**. When we mention a row or column of the table, we mean a row or column of the body of the table. The diagonal of the table that goes from the top left to the bottom right, as shown in Figure 43, is called the **main diagonal** (also known as the **leading diagonal**). It contains the results of composing each element with itself.

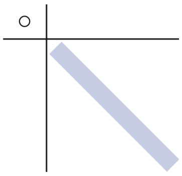


Figure 43 The main diagonal of a Cayley table

A Cayley table will help you check group axioms G1 (closure), G3 (identity) and G4 (inverses). However, group axiom G2 (associativity) is time-consuming to check from a Cayley table, so it is best to check it using a known property of the binary operation, if possible.

The next worked exercise demonstrates how to use a Cayley table to check the group axioms for a small finite set. Immediately after the worked exercise there are two propositions whose proofs clarify why the methods used to check axioms G3 (identity) and G4 (inverses) actually do check these axioms.

Worked Exercise B12

By using a Cayley table, determine whether $(\mathbb{Z}_4, +_4)$ is a group.

Solution

Construct a Cayley table for $(\mathbb{Z}_4, +_4)$.

A Cayley table for $(\mathbb{Z}_4, +_4)$ is as follows.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

We now check the group axioms.

G1 Closure

Check that every element in the body of the table belongs to the set that we are considering.

Every element in the body of the table is in $\mathbb{Z}_4$, so $\mathbb{Z}_4$ is closed under $+_4$.

G2 Associativity

Associativity is time-consuming to check from the table, but we already know that the binary operation here is associative.

Modular addition is associative.

G3 Identity

Check that there is an element such that the row labelled by that element and the column labelled by that element repeat the table borders. If there is such an element, then it is an identity element.

The row and column labelled 0 repeat the table borders, so 0 is an identity element for $+_4$ on $\mathbb{Z}_4$.

G4 Inverses

To find inverses, look for occurrences of the identity element in the body of the table.

- If it appears on the main diagonal, then the corresponding element in the table borders is self-inverse (the inverse of itself).
- If it appears off the main diagonal, but symmetrically with respect to the main diagonal, then the two corresponding elements in the table borders are inverses of each other.

In the case here, the identity element is 0 and its occurrences are as shown below.

$+_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

The identity element 0 appears on the main diagonal in the row and column labelled 0. So 0 is self-inverse.

The identity element 0 also appears on the main diagonal in the row and column labelled 2. So 2 is self-inverse.

Finally, the identity element 0 appears symmetrically in the row labelled 1 and column labelled 3, and in the row labelled 3 and column labelled 1. So 1 and 3 are inverses of each other.

So each element has an inverse in $\mathbb{Z}_4$ with respect to $+_4$.

Hence $(\mathbb{Z}_4, +_4)$ satisfies the four group axioms, and so is a group.

The proposition below justifies the method we used in Worked Exercise B12 for checking axiom G3 (identity).

Proposition B6 Checking a Cayley table for an identity

Let G be a finite set and let $\circ$ be a binary operation on G. Then the element e of G is an identity element for $\circ$ on G if and only if the row and column labelled e both repeat the table borders.

Proof In the Cayley table for $(G, \circ)$, the row labelled e contains all the composites of the form $e \circ g$, for $g \in G$, and the column labelled e contains all the composites of the form $g \circ e$, for $g \in G$.

So saying that the row labelled e repeats the top border is the same as saying that $e \circ g = g$ for all $g \in G$, and saying that the column labelled e repeats the side border is the same as saying that $g \circ e = g$ for all $g \in G$. (This is illustrated in Figure 44.)

In summary, saying that the row and column labelled e repeat the table borders is equivalent to saying that $g \circ e = g = e \circ g$ for all $g \in G$. That is, it is equivalent to saying that e is an identity element for G. ■

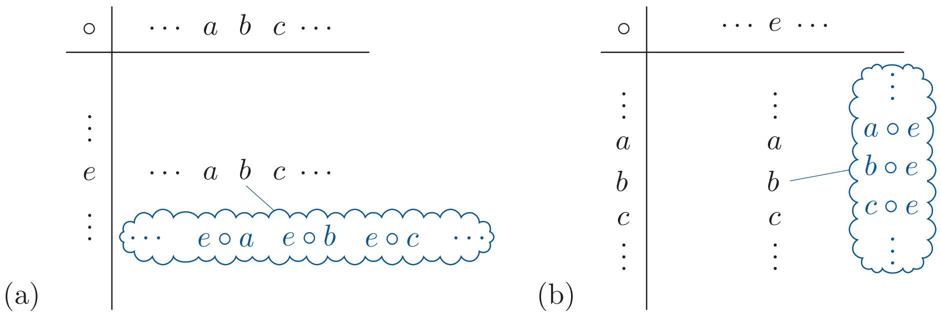


Figure 44 A row and column that repeat the table borders

The next proposition justifies the method we used for checking axiom G4 (inverses) in Worked Exercise B12.

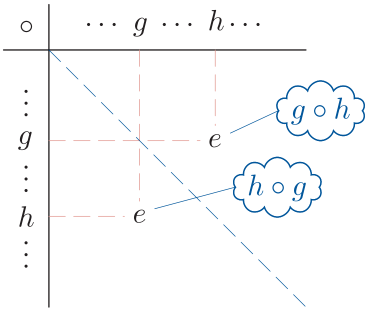


Figure 45 A Cayley table in which $g \circ h = e = h \circ g$

Proposition B7 Checking a Cayley table for inverses

Let G be a finite set, let $\circ$ be a binary operation on G and let e be an identity element for $\circ$ on G. Then the element h of G is an inverse of the element g of G if and only if e appears in the position that is in the row labelled g and column labelled h, and also in the position that is in the row labelled h and column labelled g (as shown in Figure 45).

Proof In the Cayley table, the element in the row labelled g and column labelled h is $g \circ h$, and the element in the row labelled h and column labelled g is $h \circ g$.

Saying that both these elements are equal to e is the same as saying that

$$g \circ h = e = h \circ g.$$

That is, it is equivalent to saying that h is an inverse of g. ■

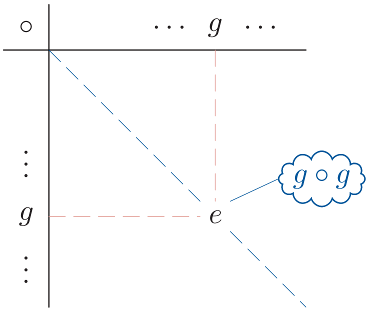


Figure 46 A Cayley table in which $g \circ g = e$

Note that, in Proposition B7 and its proof above, g and h may be the *same* element, in which case the two positions mentioned are actually the same position, namely the position that is in the row labelled g and column labelled g, as shown in Figure 46. If e appears in this position then g (equal to h) is *self-inverse*, that is, the inverse of itself.

For convenience, here is a summary of what you have seen about identifying the inverses of elements from a Cayley table.

Identifying inverses from a Cayley table

In a Cayley table for a set G and binary operation $\circ$ on G with an identity element e:

- wherever e occurs on the main diagonal, the corresponding element in the table borders is self-inverse
- wherever e occurs symmetrically with respect to the main diagonal, the corresponding elements in the table borders are inverses of each other.

These situations are illustrated in Figures 46 and 45, respectively.

The next worked exercise provides another demonstration of how to use a Cayley table to check the group axioms. In this worked exercise, the set and binary operation turn out not to form a group.

Worked Exercise B13

By using a Cayley table, determine whether $(\mathbb{Z}_4, \times_4)$ is a group.

Solution

We construct a Cayley table for $(\mathbb{Z}_4, \times_4)$:

$\times_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

We now check the group axioms.

G1 Closure

Every element in the body of the table is in $\mathbb{Z}_4$, so $\mathbb{Z}_4$ is closed under multiplication.

G2 Associativity

Modular multiplication is associative.

G3 Identity

The row and column labelled 1 repeat the table borders, so 1 is an identity element for $\times_4$ on $\mathbb{Z}_4$. (The table also shows that there is no other possible identity element.)

G4 Inverses

Look for the occurrences of the identity element 1 in the body of the table. It does not occur at all in the row labelled 0, so there is no element $x \in \mathbb{Z}_4$ such that $0 \times_4 x = 1$.

The identity element 1 does not occur in the row labelled 0, so 0 has no inverse.

Hence axiom G4 fails.

It follows that $(\mathbb{Z}_4, \times_4)$ is not a group.

In general, for group axiom G4 (inverses) to be satisfied, each row must contain an occurrence of the identity element e (this ensures that for each element g there is an element h such that $g \circ h = e$), and this occurrence of e must either be on the main diagonal or appear symmetrically with another occurrence of e, with respect to the main diagonal (this ensures that whenever we have $g \circ h = e$, we also have $h \circ g = e$). (An alternative to checking that each row contains an occurrence of e is to check that each column does.)

The methods that you have seen for checking the group axioms from a Cayley table can be summarised as follows.

Using a Cayley table to check the group axioms

Let G be a finite set and let $\circ$ be a binary operation defined on G. Then $(G, \circ)$ is a group if and only if the Cayley table for $(G, \circ)$ has the following properties.

G1 Closure The table contains only elements of the set G; that is, no new elements appear in the body of the table.

G2 Associativity The operation $\circ$ is associative. (This property is not easy to check from a Cayley table.)

G3 Identity A row and a column labelled by the same element repeat the table borders. This element is an identity element, e say.

G4 Inverses Each row contains the identity element e, occurring either on the main diagonal or symmetrically with another occurrence of e, with respect to the main diagonal. (For each such occurrence of e, the corresponding elements in the table borders are inverses of each other.)

In the next exercise you can practise using Cayley tables to check the group axioms.

Exercise B21

By first constructing a Cayley table in each case, determine which of the following are groups.

(a) $(\mathbb{Z}_5, +_5)$ (b) $(\mathbb{Z}_5, \times_5)$

(c) $(\mathbb{Z}_5 - \{0\}, \times_5) = (\{1, 2, 3, 4\}, \times_5)$

(d) $(\mathbb{Z}_6 - \{0\}, \times_6) = (\{1, 2, 3, 4, 5\}, \times_6)$

(e) $(\{2, 4, 6, 8\}, \times_{10})$ (f) $(\{1, -1\}, \times)$

Now suppose that you are presented with a Cayley table with some abstract symbols in it, such as the following:

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	c	d	e
b	b	c	d	e	a
c	c	d	e	a	b
d	d	e	a	b	c

A Cayley table like this defines a set, namely the set of elements that appear in the table borders, and it defines a binary operation on that set, since the table tells us the result of composing any two elements of the set, in either order. So we can ask whether the set and the binary operation form a group.

As you have seen, you can use the Cayley table to check group axioms G1 (closure), G3 (identity) and G4 (inverses). For the Cayley table above, all the entries in the body of the table are elements of the original set $\{e, a, b, c, d\}$, so axiom G1 (closure) holds. Also, the row and column labelled by the element e repeat the table borders, so e is an identity element. That is, axiom G3 (identity) holds. Notice that e is the only possible identity element. The occurrences of the identity element in the body of the table tell us that e is self-inverse, that a and d are inverses of each other, and that b and c are inverses of each other. So axiom G4 (inverses) holds. That leaves just axiom G2 (associativity) to be checked. Unfortunately, there is no easy way to check this axiom, other than the obvious one of going through all the ways of combining three elements. If you were to do this (and it would take rather a long time!), then you would find that the binary operation defined by the Cayley table above is in fact associative. So the abstract Cayley table above is the Cayley table of a group.

However, it is possible for a Cayley table to satisfy axioms G1 (closure), G3 (identity) and G4 (inverses), but for the operation defined by the table *not* to be associative. Here is an example:

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	e	c	d	b
b	b	d	e	a	c
c	c	b	d	e	a
d	d	c	a	b	e

You can check in the usual ways that axioms G1 (closure), G3 (identity) and G4 (inverses) are all satisfied by this Cayley table. But axiom G2 (associativity) fails, because, for example, the two expressions $b \circ (c \circ d)$ and $(b \circ c) \circ d$ give different answers:

$$b \circ (c \circ d) = b \circ a = d,$$

$$(b \circ c) \circ d = a \circ d = b.$$

This example shows that you certainly cannot determine whether a given set and binary operation form a group only by using a Cayley table to help you check group axioms G1, G3 and G4. You do also need a means of checking group axiom G2 (associativity).

Exercise B22

Given that the binary operation $\circ$ defined by the following Cayley table is associative, show that the set of elements in the table is a group under $\circ$.

$\circ$	a	b	c	d	e	f	g	h
a	f	e	g	h	a	b	d	c
b	e	f	h	g	b	a	c	d
c	h	g	f	e	c	d	b	a
d	g	h	e	f	d	c	a	b
e	a	b	c	d	e	f	g	h
f	b	a	d	c	f	e	h	g
g	c	d	a	b	g	h	f	e
h	d	c	b	a	h	g	e	f

Finally in this subsection, note that the definition of a group given in some other texts may look a little different from the definition that you have met in this module, even though the mathematical structure being defined is the same. In particular, in some texts our axiom G1 (closure) is part of the definition of a binary operation on a set, and hence is omitted from the list of group axioms.

You might also like to note that it can be proved that if group axioms G1 (closure) and G2 (associativity) hold for a set and binary operation $(G, \circ)$, then to check that group axioms G3 (identity) and G4 (inverses) also hold it is enough to show that

- there is an element e in G such that $g \circ e = g$ for all g in G, and
- for each element g in G, there is an element h in G such that $g \circ h = e$.

That is, you do not also have to show that $e \circ g = g$ for all g in G, or that for each element g in G the element h in G that satisfies $g \circ h = e$ also satisfies $h \circ g = e$. So the group axioms that you have met in this unit can be reduced to a more minimal set of axioms. However, in practice it is convenient to work with the set of group axioms stated earlier, and we will continue to do so throughout this module.

The origins of group theory

Group theory arose historically from three different areas of study: number theory, the theory of algebraic equations, and geometry.

The study of modular arithmetic that was introduced by Carl Friedrich Gauss in his *Disquistiones Arithmeticae* of 1801 contains elements that we would nowadays recognise as group theory. At about the same time, many mathematicians, including Joseph-Louis Lagrange (1736–1813), Paolo Ruffini (1765–1822), Augustin-Louis Cauchy (1789–1857) and Évariste Galois (1811–1832) worked on the question of which polynomial equations could be solved algebraically, and it gradually became apparent that the key to answering this question lay in considering groups of *permutations*, which you will meet in Unit B3 *Permutations*. In 1872, Felix Klein (1849–1925) in his *Erlangen Program*, a review of contemporary methods in geometry, used group theoretic methods to classify the different geometries, such as Euclidean, hyperbolic, and projective geometry, and a few years later Henri Poincaré (1854–1912) pioneered the introduction of group theoretic and geometric methods into complex function theory, these ideas becoming hugely significant in modern mathematics. One of the main instigators of the abstraction of the similar ideas in these different contexts into modern group theory was Arthur Cayley (1821–1895), around the middle of the 19th century.

In 1870 Camille Jordan (1838–1922) published his monumental treatise on permutation groups, and by around the end of the century textbooks on abstract group theory were being published, two of the most important being those by William Burnside and Heinrich Weber. Today, group theory remains a major area of mathematical research.

3.4 Standard groups of numbers

In this subsection you will meet some standard groups of numbers. They include many of the groups of numbers that you met in the previous two subsections.

Infinite groups of numbers

In Subsection 3.2 you saw that the sets $\mathbb{Z}$ and $\mathbb{R}$, with addition, are groups, and that the sets $\mathbb{Q}^*$ and $\mathbb{R}^*$, with multiplication, are groups. It can be shown in similar ways that the sets $\mathbb{Q}$ and $\mathbb{C}$, with addition, are groups, and that the set $\mathbb{C}^*$, with multiplication, is a group. (As you may guess, the notation $\mathbb{C}^*$ denotes the set $\mathbb{C} - \{0\}$ of all complex numbers except 0.)

In fact, you saw (without proof) in Unit A2 that the sets $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$, with addition and multiplication, are *fields*, and it follows from this that $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \times)$, $(\mathbb{R}^*, \times)$ and $(\mathbb{C}^*, \times)$ are all groups. So we have the facts below.

Some standard infinite groups of numbers

The following are groups:

$$\begin{array}{llll} (\mathbb{Z}, +), & (\mathbb{Q}, +), & (\mathbb{R}, +), & (\mathbb{C}, +), \\ & (\mathbb{Q}^*, \times), & (\mathbb{R}^*, \times), & (\mathbb{C}^*, \times). \end{array}$$

Groups from modular arithmetic

In Worked Exercise B12 and Exercise B21 in Subsection 3.3 you saw that $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5, +_5)$ are groups. In fact, we have the following general result.

Theorem B8

For each integer $n \geq 2$, the set $\mathbb{Z}_n$ is a group under $+_n$.

Proof The four group axioms hold because they are properties A1–A4 of addition in $\mathbb{Z}_n$, which you met in Subsection 3.3 of Unit A2. ■

You also saw in Exercise B21 that $(\mathbb{Z}_5, \times_5)$ is not a group. In general, $(\mathbb{Z}_n, \times_n)$ is not a group for any positive integer n, because 0 has no inverse with respect to $\times_n$. This type of situation has arisen before: you saw in Subsection 3.3 that $(\mathbb{R}, \times)$ is not a group, because 0 has no inverse with respect to ×. You also saw that the set $\mathbb{R}^* = \mathbb{R} - \{0\}$ *is* a group under ×, and so are the sets $\mathbb{Q}^* = \mathbb{Q} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$. However, removing the integer 0 from the set $\mathbb{Z}_n$ does not necessarily give a group under $\times_n$: you saw in Exercise B21 that $(\{1, 2, 3, 4\}, \times_5)$ is a group, but $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group.

One reason why removing 0 from $\mathbb{Z}_n$ does not necessarily give a group under $\times_n$ is that, as you saw in Subsection 3.4 of Unit A2, in the set $\mathbb{Z}_n$ only the integers coprime to n have inverses with respect to $\times_n$; the other integers do not. So $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group because the integer 2, for instance, is not coprime to 6 and so does not have an inverse with respect to $\times_6$ in $\mathbb{Z}_6$; axiom G4 therefore fails. (Axiom G1 also fails: for example, $2, 3 \in \{1, 2, 3, 4, 5\}$, but $2 \times_6 3 = 0 \notin \{1, 2, 3, 4, 5\}$.)

It turns out, however, that if you remove not only the integer 0 from $\mathbb{Z}_n$, but also all the other integers in $\mathbb{Z}_n$ that do not have inverses with respect to $\times_n$, then you *do* obtain a group under $\times_n$. This is proved below. The subset of $\mathbb{Z}_n$ that you are left with is the set of all the integers in $\mathbb{Z}_n$ that are coprime to n, and we denote this set by U_n. For example, the set of integers in $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ that are coprime to 5 is

$$U_5 = \{1, 2, 3, 4\},$$

and this set forms a group under $\times_n$, as you saw in Exercise B21. Similarly, the set of integers in $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$ that are coprime to 6 is

$$U_6 = \{1, 5\},$$

and this set forms a group under $\times_6$. It has Cayley table

$\times_6$	1	5
1	1	5
5	5	1

and both of its elements are self-inverse. (The U in the notation U_n is for *units*, which means ‘elements that have multiplicative inverses’, but we will not need to use this term in this module.)

Here is the general result.

Theorem B9

For each integer $n \geq 2$, the set U_n of all integers in $\mathbb{Z}_n$ that are coprime to n is a group under $\times_n$.

Proof We show that the four group axioms hold for $(U_n, \times_n)$. Throughout the proof, we make use of the properties of integers in $\mathbb{Z}_n$ that you met in Unit A2.

G1 Closure

Let $a, b \in U_n$; then both a and b are coprime to n. To prove that $a \times_n b \in U_n$, we have to show that $a \times_n b$ is coprime to n.

To do this, we show that $a \times_n b$ has a multiplicative inverse in $\mathbb{Z}_n$. By Theorem A9 in Unit A2, since both a and b are coprime to n, they both have multiplicative inverses in $\mathbb{Z}_n$, say c and d, respectively. Now

$$(c \times_n d) \times_n (a \times_n b) = (c \times_n a) \times_n (d \times_n b) = 1 \times_n 1 = 1,$$

and similarly

$$(a \times_n b) \times_n (c \times_n d) = 1.$$

Hence $c \times_n d$ is a multiplicative inverse of $a \times_n b$ in $\mathbb{Z}_n$.

It now follows from Theorem A9 in Unit A2 that $a \times_n b$ is coprime to n, so $a \times_n b \in U_n$. Thus U_n is closed under $\times_n$.

G2 Associativity

Modular multiplication is associative.

G3 Identity

We have $1 \in U_n$, since 1 is coprime to n, and, for all $a \in U_n$,

$$a \times_n 1 = a = 1 \times_n a.$$

So 1 is an identity element for $\times_n$ on U_n.

G4 Inverses

Let $a \in U_n$; then a is coprime to n. By Theorem A9 in Unit A2, a has a multiplicative inverse b in $\mathbb{Z}_n$. We have to show that $b \in U_n$; that is, we have to show that b is coprime to n. Since a and b satisfy the equations

$$a \times_n b = 1 = b \times_n a,$$

the number a is also a multiplicative inverse of b in $\mathbb{Z}_n$, and hence, also by Theorem A9 in Unit A2, b is coprime to n. So $b \in U_n$. Thus a has an inverse with respect to $\times_n$ in U_n.

Hence $(U_n, \times)$ satisfies the four group axioms, and so is a group. ■

If n is a prime number, then *all* the non-zero integers in $\mathbb{Z}_n$ are coprime to n, so in this case simply removing the integer 0 from $\mathbb{Z}_n$ *does* give a group. For example, $(\{1,2,3,4\},\times_5)$ is a group, as mentioned above, because 1, 2, 3 and 4 are all coprime to 5.

So Theorem B9 has the following corollary. In this corollary, and in general, we use the notation $\mathbb{Z}_p^*$ to denote the set of all non-zero integers in $\mathbb{Z}_p$.

Corollary B10

If p is a prime number, then $(\mathbb{Z}_p^*,\times_p)$ is a group.

For example, $(\mathbb{Z}_5^*,\times_5)$, $(\mathbb{Z}_7^*,\times_7)$ and $(\mathbb{Z}_{19}^*,\times_{19})$ are groups, since 5, 7 and 19 are prime. Notice that, for any prime number p, the notations $(\mathbb{Z}_p^*,\times_p)$, $(U_p,\times_p)$ and $(\{1,2,\dots,p-1\},\times_p)$ all denote the same group. However, we usually use the notation $(\mathbb{Z}_p^*,\times_p)$ when p is prime.

Note that, since $+_n$ and $\times_n$ are commutative operations, all the groups described in Theorems B8 and B9, and in Corollary B10, are abelian.

Exercise B23

For each of the following groups, construct a Cayley table and write down the inverse of each element.

(a) $(\mathbb{Z}_7,+_7)$ (b) $(\mathbb{Z}_7^*,\times_7)$ (c) $(U_{10},\times_{10})$ (d) $(U_9,\times_9)$

Theorems B8 and B9 and Corollary B10 do not describe all the groups that come from modular arithmetic: there are many others. For example, in Exercise B21 you saw that $(\{2,4,6,8\},\times_{10})$ is a group; notice that this group does not contain the integer 1 and so its identity element is not 1.

4 Deductions from the group axioms

The advantage of defining a group $(G,\circ)$ as a general set G and a general binary operation $\circ$ on G that together satisfy the four group axioms G1–G4 is that anything that we can prove directly from the axioms (in the general case) must apply to any group (any specific case). Thus, by giving one proof, we can simultaneously establish a result that holds for groups of symmetries, infinite groups of real or complex numbers, modular arithmetic groups, and many more groups.

In this section you will meet some important basic properties of groups that can be deduced from the group axioms. The proofs in this section, showing how the deductions are made, are short and elegant. You should read them and try to understand them, to improve your knowledge of group theory and your understanding of how mathematical results are proved. However, be assured that a beginner in group theory is unlikely to think of these proofs unaided. Although you will be asked to prove some results in group theory yourself, and your understanding of the proofs in this section will help you with that, the proofs that you will be asked to produce will be more suitable for a beginner.

4.1 Basic properties of groups

Let us start with a reminder of the group axioms.

Definition

Let G be a set and let $\circ$ be a binary operation defined on G. Then $(G, \circ)$ is a **group** if the following four axioms hold.

G1 Closure For all g, h in G,

$$g \circ h \in G.$$

G2 Associativity For all g, h, k in G,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

G3 Identity There is an element e in G such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for $\circ$ on G.)

G4 Inverses For each element g in G, there is an element h in G such that

$$g \circ h = e = h \circ g.$$

(The element h is an **inverse element** of g with respect to $\circ$.)

Before we go on to look at some deductions that we can make from the group axioms, it is important for you to understand what axiom G2 (associativity) tells us about the binary operation $\circ$ of a group $(G, \circ)$.

It tells us that even though the binary operation of a group is a means of combining *two* group elements, we can write a composite of *three* group elements without using brackets. For example, if g, h and k are elements of a group $(G, \circ)$, then we can write

$$g \circ h \circ k,$$

rather than either

$$(g \circ h) \circ k \quad \text{or} \quad g \circ (h \circ k).$$

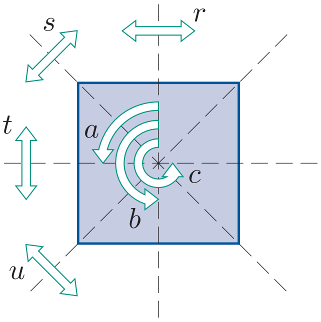


Figure 47 $S(\square)$

This is because axiom G2 guarantees that both possible interpretations of $g \circ h \circ k$ give the same answer. We can evaluate $g \circ h \circ k$ by using either interpretation.

You saw this illustrated for the group $S(\square)$ in Subsection 1.2: you saw there that, with our standard labelling for the symmetries of the square (shown again in Figure 47), we can evaluate the composite $b \circ a \circ t$ in either of the following two ways, obtaining the same answer:

$$b \circ (a \circ t) = b \circ u = s,$$
$$(b \circ a) \circ t = c \circ t = s.$$

In fact axiom G2 tells us more: it tells us that we can write a composite of *any finite number* of group elements with no brackets, without there being any ambiguity about the meaning of the expression. For example, if a, b, c and d are elements of a group $(G, \circ)$, then we can write the composite

$$a \circ b \circ c \circ d$$

of four group elements without brackets. To see why, notice that there are various ways in which we can 'bracket' this expression to indicate which elements are being composed with which, such as

$$(a \circ b) \circ (c \circ d),$$
$$a \circ \big(b \circ (c \circ d)\big),$$
$$a \circ \big((b \circ c) \circ d\big),$$
$$\big(a \circ (b \circ c)\big) \circ d,$$

and so on. The first two expressions here are equal, because applying axiom G2 to the three group elements a, b and $c \circ d$ (in that order) gives

$$(a \circ b) \circ (c \circ d) = a \circ \big(b \circ (c \circ d)\big).$$

Similarly, the second and third expressions are equal, because applying axiom G2 to the three group elements b, c and d (in that order) gives

$$a \circ \big(b \circ (c \circ d)\big) = a \circ \big((b \circ c) \circ d\big).$$

In this manner, by repeatedly applying axiom G2, we can show that any way of bracketing the expression is equal to any other way. So all the different ways of bracketing the expression give the same answer, and hence we can write the expression with no brackets, without there being any ambiguity about its meaning.

We can evaluate a composite of group elements such as $a \circ b \circ c \circ d$ by bracketing it however we wish, *provided that we do not change the order in which the elements appear.*

Now let us look at some of the basic properties of groups that can be deduced from the group axioms.

Uniqueness properties

Each of the examples of groups that you have seen has contained precisely *one* identity element. In fact this is always the case, as stated and proved below. We say that the identity element in a group is *unique*.

There is a standard method that is often helpful for proving uniqueness, and we use it in the proof below. The idea is that, to prove that there can be only one identity element in a group, we suppose that e and e', say, both represent identity elements, and prove that the only possibility is that e and e' are in fact the same element. You can often use a similar technique to prove uniqueness in other situations, and in fact we will use the same technique in the next proof too.

Proposition B11

In any group, the identity element is unique.

Proof Let $(G, \circ)$ be a group, and suppose that e and e' are identity elements in this group. We have to show that $e = e'$.

Consider the expression $e \circ e'$. Since e is an identity element, the result of composing e with any other element, in either order, is simply that other element (by axiom G3). So we must have

$$e \circ e' = e'.$$

Similarly, since e' is an identity element, we must have

$$e \circ e' = e.$$

It follows that

$$e = e',$$

as required. ■

Because of Proposition B11, we can, and shall, refer to *the* identity element of a group.

We now look at another uniqueness property. In each of the examples of groups that you have seen, every element has precisely one inverse. Again, this is always the case in a group, as proved below.

Proposition B12

In any group, each element has a unique inverse.

Proof Let $(G, \circ)$ be a group with identity element e, let g be any element in this group, and suppose that g has inverse elements x and y. We have to show that $x = y$.

Consider the expression $y \circ g \circ x$. Since x is an inverse of g, we have

$$\begin{aligned} y \circ g \circ x &= y \circ (g \circ x) \quad \text{(by axiom G2, associativity)} \\ &= y \circ e \quad \text{(by axiom G4, inverses)} \\ &= y \quad \text{(by axiom G3, identity).} \end{aligned}$$

On the other hand, since y is an inverse of g, we have

$$\begin{aligned} y \circ g \circ x &= (y \circ g) \circ x \quad \text{(by axiom G2, associativity)} \\ &= e \circ x \quad \text{(by axiom G4, inverses)} \\ &= x \quad \text{(by axiom G3, identity).} \end{aligned}$$

It follows that $x = y$, as required. ■

Because of Proposition B12, we can, and shall, refer to *the* inverse of a group element. This property also allows us to use the following notation for inverses in a group.

Notation

Let g be an element of a group $(G, \circ)$. Then we denote the inverse of g by g^{-1}. So

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

In fact, the two proofs above are not the first time that you have met the standard method for proving uniqueness. For example, you saw in Unit A1 how to use this method to prove that a function is one-to-one. To prove that a function f is one-to-one, essentially you have to show that for every element y in the image set of f, there is a *unique* element x in the domain of f such that $f(x) = y$. You saw that to do this, the standard method is to suppose that x_1 and x_2, say, both represent elements that are mapped by f to y, and prove that the only possibility is that x_1 and x_2 are in fact the same element.

Also, in Unit A2 the standard method for proving uniqueness was used to prove that, in the system $\mathbb{Z}_n$ with addition and multiplication modulo n, if an element *has* a multiplicative inverse then that multiplicative inverse is unique. The proof of that result is essentially the same as the proof of Proposition B12 above.

Properties of inverse elements

We now turn to some properties of inverse elements in groups.

In the examples of groups that you have seen, some elements are self-inverse, and the remaining elements can be arranged into pairs of elements that are inverses of each other. So, in all the examples, if g is a group element with inverse g^{-1}, then the inverse of g^{-1} is g. This is always the case in a group, as stated and proved below.

Proposition B13

Let g be an element of a group $(G, \circ)$. Then

the inverse of g^{-1} is g,

that is,

$$(g^{-1})^{-1} = g.$$

Proof By axiom G4, since g has inverse g^{-1},

$$g \circ g^{-1} = e = g^{-1} \circ g.$$

We can write these equations in a different order as

$$g^{-1} \circ g = e = g \circ g^{-1}.$$

This tells us that g is an inverse of g^{-1}. Hence, by Proposition B12 (uniqueness of the inverse of a group element), g is *the* inverse of g^{-1}; that is, we have

$$(g^{-1})^{-1} = g.$$ ■

Our second property of inverses concerns the inverse of a composite of two group elements.

Proposition B14

Let x and y be elements of a group $(G, \circ)$. Then

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

Proof We start by showing that $y^{-1} \circ x^{-1}$ is an inverse of $x \circ y$. To do this, we have to show that

$$(x \circ y) \circ (y^{-1} \circ x^{-1}) = e = (y^{-1} \circ x^{-1}) \circ (x \circ y).$$

Now

$$\begin{aligned}(x \circ y) \circ (y^{-1} \circ x^{-1}) &= x \circ (y \circ y^{-1}) \circ x^{-1} \\ &\qquad \text{(by axiom G2, associativity)} \\ &= x \circ e \circ x^{-1} \quad \text{(by axiom G4, inverses)} \\ &= x \circ x^{-1} \quad \text{(by axiom G3, identity)} \\ &= e \quad \text{(by axiom G4, inverses),}\end{aligned}$$

and

$$\begin{aligned}(y^{-1} \circ x^{-1}) \circ (x \circ y) &= y^{-1} \circ (x^{-1} \circ x) \circ y \\ &\qquad \text{(by axiom G2, associativity)} \\ &= y^{-1} \circ e \circ y \quad \text{(by axiom G4, inverses)} \\ &= y^{-1} \circ y \quad \text{(by axiom G3, identity)} \\ &= e \quad \text{(by axiom G4, inverses).}\end{aligned}$$

Hence $y^{-1} \circ x^{-1}$ is an inverse of $x \circ y$. So, by Proposition B12 (uniqueness of the inverse of a group element), $y^{-1} \circ x^{-1}$ is *the* inverse of $x \circ y$; that is,

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$ ■

Proposition B14 is a general property that holds for all inverses of composites (not just in group theory). For example, if f and g are functions that have inverses (that is, if they are one-to-one functions), then $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

Here is one way to see that the different orders of composition on the two sides of equations like this makes sense. Consider the composite action of first putting your socks on and then putting your shoes on. To carry out the inverse of this action, you first take your shoes off and then take your socks off!

Proposition B14 extends to composites of more than two group elements. For example, if x, y and z are elements of a group $(G, \circ)$, then

$$(x \circ y \circ z)^{-1} = z^{-1} \circ y^{-1} \circ x^{-1}.$$

This follows from Proposition B14, as follows:

$$\begin{aligned}(x \circ y \circ z)^{-1} &= (y \circ z)^{-1} \circ x^{-1} \quad \text{(by Proposition B14)} \\ &= z^{-1} \circ y^{-1} \circ x^{-1} \quad \text{(by Proposition B14 again).}\end{aligned}$$

By repeatedly applying Proposition B14 in this way, we can extend it to a composite of any finite number of group elements.

Our final properties in this subsection, in the box below, do not explicitly involve inverses, but are proved using inverses. These properties will be familiar to you from elementary arithmetic, in the cases where the binary operation is addition or multiplication. For example, suppose that a and b are real numbers, and that $a + 3 = b + 3$. Both sides of this equation involve adding the same real number (here, 3) to another real number, so we know that we can *cancel* the 3 that occurs on both sides of the equation and conclude that $a = b$. Similarly, if $5a = 5b$ we can cancel the 5 that multiplies the real numbers a and b, and again conclude that $a = b$.

These properties are known as *cancellation laws*. They apply in any group, as stated below.

Proposition B15 Cancellation Laws

In any group $(G, \circ)$ with elements a, b and x:

- if $x \circ a = x \circ b$, then $a = b$ (**Left Cancellation Law**)
- if $a \circ x = b \circ x$, then $a = b$ (**Right Cancellation Law**).

Proof Here is a proof of the Left Cancellation Law. Suppose that, in a group $(G, \circ)$,

$$x \circ a = x \circ b.$$

Composing both sides on the left with the inverse of x, we obtain

$$x^{-1} \circ x \circ a = x^{-1} \circ x \circ b.$$

By axiom G2 (associativity), this gives

$$(x^{-1} \circ x) \circ a = (x^{-1} \circ x) \circ b.$$

Hence, by axiom G4 (inverses), we obtain

$$e \circ a = e \circ b,$$

and therefore, by axiom G3 (identity),

$$a = b.$$

You are asked to prove the Right Cancellation Law in the next exercise. ■

Exercise B24

By adapting the proof above, prove the Right Cancellation Law for a group $(G, \circ)$, namely,

$$\text{if } a \circ x = b \circ x, \text{ then } a = b.$$

In the next two exercises, you can try your hand at proving results by using the group axioms. Do not worry if you find these exercises difficult: accept them as a challenge. Proving results in group theory can be tricky, especially when you are new to it, and there are further opportunities for you to practise it throughout Book B.

Exercise B25

Suppose that a, b and c are elements of a group $(G, \circ)$ such that $a \circ b \circ c = e$, where e is the identity element. Prove that $b \circ c \circ a = e$.

As you become more familiar with proving results in group theory, you do not need to name the group axioms explicitly every time you use them: you just need to make sure that you clearly justify the steps of your proof, using appropriate words. Your justification of a step might involve referring to a group axiom in some way, or it might be based on a result proved earlier about groups. And, of course, it may be based on something else altogether, such as a supposition that you made in order to prove an implication. In general, the amount of justification that you provide should be enough to convince a reader whose mathematical experience is about the same as yours. This will be similar to the amount of justification in comparable proofs given in the module texts and in the solutions to exercises and worked exercises.

The next exercise is a little more challenging than the one above. Treat it as a puzzle: see if you can work it out, but do not worry if you cannot.

Exercise B26

Let $(G, \circ)$ be a group. Proposition B14 tells us that

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1} \text{ for all } x, y \in G.$$

Prove that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G$$

if and only if $(G, \circ)$ is abelian. You can use any of the properties proved so far in this section.

Hint. Remember from Unit A3 *Mathematical language* that to prove a statement of the form 'A if and only if B', you have to prove both that A implies B and that B implies A.

Remember also that an *abelian* group $(G, \circ)$ is one for which $x \circ y = y \circ x$ for all $x, y \in G$.

4.2 Properties of group tables

The Cayley table of a group is called a **group table**. In this subsection we will look at some properties possessed by every group table.

In Subsection 3.3 you met some properties of group tables that correspond directly to the group axioms. For example, you saw that group axioms G1 (closure) and G3 (identity) immediately give the following two properties.

Proposition B16

In a group table, the only elements in the body of the table are those that appear in the table borders.

Proposition B17

In a group table, the row and column corresponding to the identity element repeat the table borders.

Exercise B27

Decide which is the identity element in each of the following group tables.

(a)

	O	E
O	E	O
E	O	E

(b)

	D	I
D	D	I
I	I	D

(c)

	u	v	w	x
u	w	x	u	v
v	x	w	v	u
w	u	v	w	x
x	v	u	x	w

As you have seen, if we know which element of a group is the identity element, then we usually write this element first in the borders of the group table.

Here is another property of group tables.

Proposition B18

In a group table, each element of the group occurs exactly once in each row and exactly once in each column.

Proof We prove this statement for the rows of a group table. The proof for columns is similar, and you are asked to produce it in the next exercise.

Let g be any group element; we will consider the row corresponding to g. Let h also be any group element; we will show that h occurs exactly once in this row.

This is equivalent to proving that there is *exactly one* element of the group, x say, such that

$$g \circ x = h,$$

as illustrated in Figure 48.

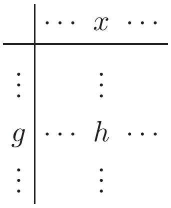


Figure 48 Element h in row g

To show that there is *at least* one such element x, let $x = g^{-1} \circ h$. Then

$$\begin{aligned} g \circ x &= g \circ g^{-1} \circ h \\ &= e \circ h \\ &= h, \end{aligned}$$

so $x = g^{-1} \circ h$ has the property $g \circ x = h$, as claimed.

To show that $x = g^{-1} \circ h$ is the *only* element x of the group such that $g \circ x = h$, we use our standard method for proving uniqueness. Suppose that x and y are group elements such that

$$g \circ x = h \quad \text{and} \quad g \circ y = h.$$

Then

$$g \circ x = g \circ y,$$

so, by the Left Cancellation Law,

$$x = y.$$

So there is indeed exactly one element x of the group such that $g \circ x = h$, namely $x = g^{-1} \circ h$.

In other words, in the row labelled g, the element h appears exactly once; it appears in the column labelled by the element $g^{-1} \circ h$. ■

Exercise B28

By adapting the proof above, prove the second part of Proposition B18; that is, prove that in a group table each element of the group occurs exactly once in each column.

Proposition B18 tells us, in particular, that the identity element e occurs exactly once in each row and each column of a group table. By what you saw in Subsection 3.3 about checking the group axioms from a Cayley table, this single occurrence of e in each row (or column) must appear either on the main diagonal or symmetrically with another occurrence of e, with respect to the main diagonal, as illustrated in Figure 49.

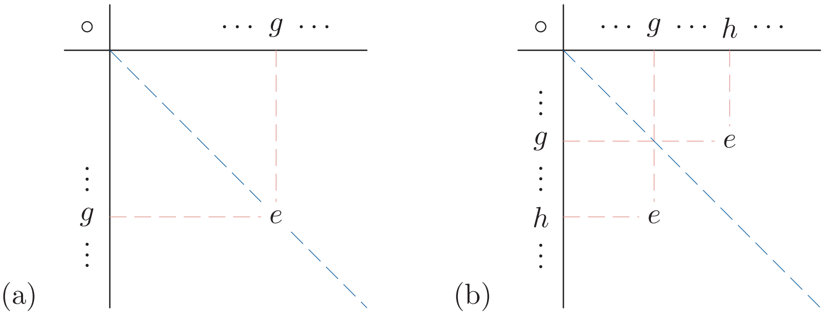


Figure 49 The occurrence of the identity element e in row g (a) if g is self-inverse (b) if g has inverse $h \neq g$

So *all* occurrences of the identity element e in a group table must appear symmetrically with respect to the main diagonal. This property is stated slightly more concisely below.

Proposition B19

In a group table, the identity element e occurs symmetrically with respect to the main diagonal.

Exercise B29

In each of the Cayley tables below, the identity element e occurs in each row and column, but the table is not a group table. Explain how you can tell this.

(a)

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	e	c	d	a
c	c	d	e	a	b
d	d	c	a	b	e

(b)

$\circ$	e	a	b	c	d
e	e	a	b	c	d
a	a	b	d	e	c
b	b	d	c	d	e
c	c	e	d	a	b
d	d	c	e	b	a

Finally in this subsection, we consider a property that *only some* group tables have.

Notice that, for any elements g and h of a group G, the entries in the group table corresponding to the composites $g \circ h$ and $h \circ g$ are placed symmetrically with respect to the main diagonal, as illustrated in Figure 50. Thus we have the following result.

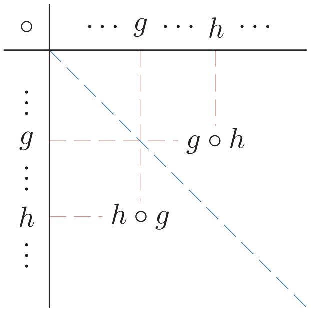


Figure 50 The positions of the composites $g \circ h$ and $h \circ g$ in a group table

Proposition B20 Group table of an abelian group

A group is abelian if and only if its group table is symmetric with respect to the main diagonal.

For example, Figure 51 shows that $(\mathbb{Z}_6, +_6)$ is an abelian group, whereas $(S(\triangle), \circ)$ is not.

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

(a) symmetric

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
s	t	r	s	a	b	e

(b) not symmetric

Figure 51 The group tables of (a) $(\mathbb{Z}_6, +_6)$ (b) $(S(\triangle), \circ)$

Exercise B30

Each of the following tables is a group table for a group of order 8 with identity e. In each case, state whether the group is abelian and draw up a table of inverses.

(a)

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	e	c	b	f	d	h	g
b	b	c	e	a	g	h	d	f
c	c	b	a	e	h	g	f	d
d	d	f	g	h	e	a	b	c
f	f	d	h	g	a	e	c	b
g	g	h	d	f	b	c	e	a
h	h	g	f	d	c	b	a	e

(b)

	e	a	b	c	d	f	g	h
e	e	a	b	c	d	f	g	h
a	a	b	c	e	f	g	h	d
b	b	c	e	a	g	h	d	f
c	c	e	a	b	h	d	f	g
d	d	h	g	f	b	a	e	c
f	f	d	h	g	c	b	a	e
g	g	f	d	h	e	c	b	a
h	h	g	f	d	a	e	c	b

5 Symmetry in $\mathbb{R}^3$

Having considered symmetries of two-dimensional figures, and seen that they form groups, we now extend the ideas to three-dimensional objects. Remember that we use the notation $\mathbb{R}^3$ to denote three-dimensional space, in which a point is specified by three coordinates x, y, z.

5.1 Symmetries of figures in $\mathbb{R}^3$

We begin by adapting to $\mathbb{R}^3$ the definitions that you met earlier relating to figures and symmetries in $\mathbb{R}^2$.

Definitions

A **figure** in $\mathbb{R}^3$ is any subset of $\mathbb{R}^3$.

A **bounded** figure in $\mathbb{R}^3$ is one that can be surrounded by a sphere (of finite radius).

A figure in $\mathbb{R}^3$ that is a shape with non-zero height, non-zero width and non-zero depth is called a **solid figure**, or just a **solid**. In this section we will mainly consider bounded solids whose faces are polygons. A solid of this type is called a **polyhedron**; some examples are shown in Figure 52. The plural of *polyhedron* is *polyhedra* or simply *polyhedrons*.

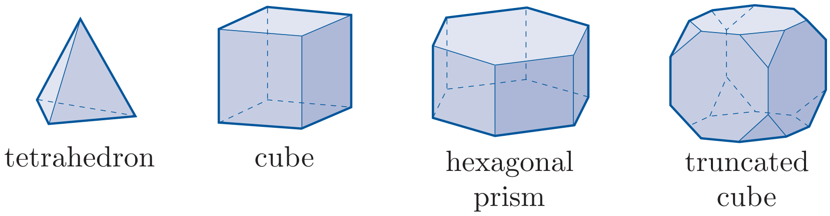


Figure 52 Four polyhedra

The word *polyhedron* derives from the Greek for ‘many faces’. Similarly, the word *polygon* derives from the Greek for ‘many angles’.

We will restrict our attention to **convex** polyhedra; that is, those without dents or dimples or spikes – in other words, those that are such that if you choose any two points that lie on different faces, then the line segment joining those points always lies inside the polyhedron, as illustrated in Figure 53.

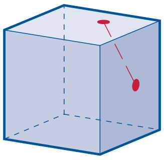


Figure 53 A cube is a convex polyhedron

Of particular interest are the **regular polyhedra** (**Platonic solids**): these are the convex polyhedra in which all the faces are congruent regular polygons and at each vertex the same number of faces meet, arranged in the same way. (Remember that two plane figures are said to be **congruent** if they are the same size and shape – that is, if you can translate, rotate and/or reflect one figure to make it fit exactly on top of the other.) There are five regular polyhedra, as shown in Figure 54. An explanation of why there are only five is given in Subsection 5.4.

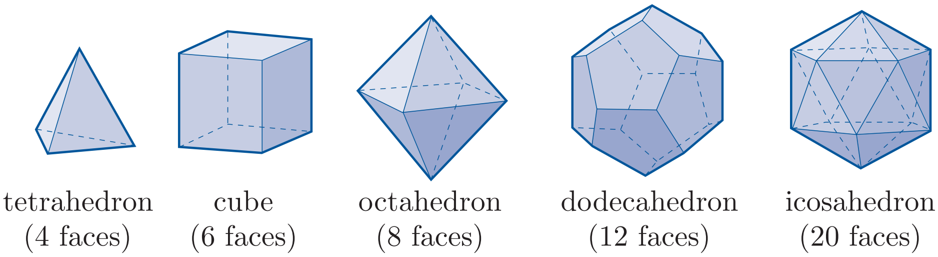


Figure 54 The five Platonic solids

The Platonic solids are so named not because Plato (427–347 BCE) discovered them, but because he associated the regular tetrahedron, cube, octahedron and icosahedron with the four elements of fire, earth, air and water, respectively; it is not completely clear with what Plato associated the dodecahedron, but he said that it ‘delineates the whole’.

The definitions of an isometry and a symmetry for $\mathbb{R}^3$ are almost exactly the same as for $\mathbb{R}^2$.

Definitions

An **isometry** of $\mathbb{R}^3$ is a function $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ that preserves distances.

A **symmetry** of a figure F in $\mathbb{R}^3$ is an isometry that maps F to itself; that is, an isometry $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^3$ such that $f(F) = F$.

Two symmetries of a figure F are **equal** if they have the same effect on F, that is, $f(X) = g(X)$ for all points $X \in F$.

The types of isometries that are potential symmetries of a bounded figure in $\mathbb{R}^3$ are the following.

- The **identity transformation**: equivalent to doing nothing to a figure.
- A **rotation**: as illustrated in Figure 55(a), it is specified by a line known as an *axis of symmetry* together with a *direction* of rotation and an *angle of rotation*.
- A **reflection**: as illustrated in Figure 55(b), it is specified by the *plane* in which the reflection takes place.
- A **composite** of isometries of the types above – which may itself be of one of the types above, or (unlike with symmetries of plane figures) may not.

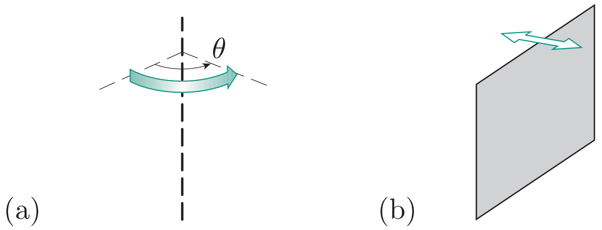


Figure 55 (a) A rotation about an axis of symmetry (b) A reflection in a plane

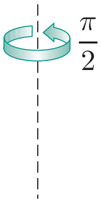


Figure 56 An arrow indicating the direction of rotation, with the angle of rotation marked

We have to be careful with rotations in $\mathbb{R}^3$, as what is clockwise when we look along a line in one direction is anticlockwise when we look along it in the other direction. We often indicate the direction of rotation by an arrow on a diagram, as in Figure 55(a). However, note that in the remainder of this section a rotation arrow in a diagram of a figure in $\mathbb{R}^3$ indicates only the *direction of rotation*, as illustrated in Figure 56, and not the *size of the angle* through which the figure is rotated. The size of the angle of rotation is sometimes marked next to the rotation arrow, as in Figure 56.

To illustrate symmetries of figures in $\mathbb{R}^3$, let us consider some symmetries of the cube.

Figure 57 shows the effect of a particular rotational symmetry of the cube, namely rotation through $\pi/2$ about the vertical line through the centre of the cube, in the direction indicated.

In diagrams such as this, the numbers have a similar purpose to the numbers that we used in diagrams of plane figures earlier. They do not label vertices: instead they label fixed locations in space, so they do not move when the figure is rotated or reflected, or transformed in any other way by a symmetry. In Figure 57, and in the next few figures, the change in the position of the cube is indicated by a dot and a small square that mark two corners of one of its faces.

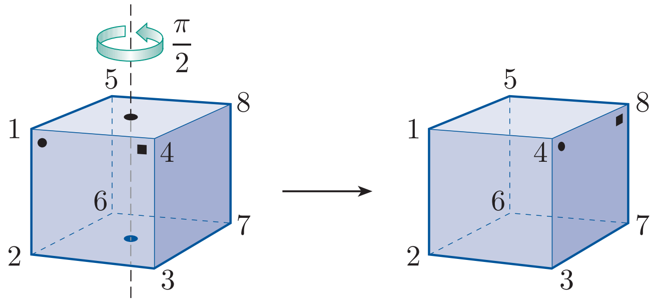


Figure 57 A rotation of the cube through $\pi/2$ about its vertical axis

We use two-line symbols to represent symmetries of figures in $\mathbb{R}^3$ in the same way as we do for plane figures. For example, with the labelling shown, the symmetry in Figure 57 is represented by

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 7 & 8 & 1 & 2 & 6 & 5 \end{pmatrix}.$$

Another symmetry of the cube is the identity symmetry, which can be thought of as a zero rotation, and is represented by

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix}.$$

Figure 58 shows a reflectional symmetry of the cube, namely reflection in the vertical plane shown.

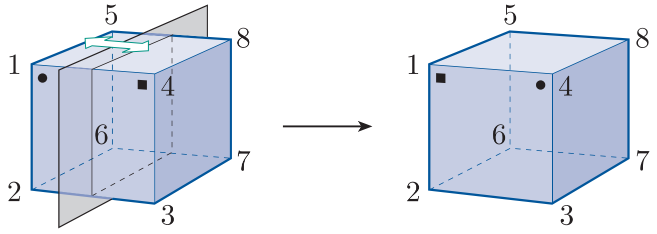


Figure 58 A reflection of the cube in a vertical plane

The two-line symbol for this reflection is

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{pmatrix}.$$

We can compose symmetries of solid figures written in two-line notation in the same way as for plane figures.

For example, the rotation in Figure 57 followed by the reflection in Figure 58 is the symmetry

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\4&3&2&1&8&7&6&5\end{pmatrix}\circ\begin{pmatrix}1&2&3&4&5&6&7&8\\4&3&7&8&1&2&6&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6&7&8\\1&2&6&5&4&3&7&8\end{pmatrix}.$$

(Remember that the symmetry on the right is the one carried out first.) This symmetry is reflection in the diagonal plane passing through the locations labelled 1, 2, 7 and 8, as shown in Figure 59.

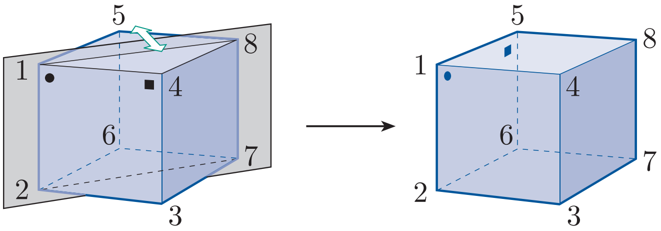


Figure 59 A reflection of the cube in a diagonal vertical plane

We can also find the inverse of a symmetry of a solid figure written in two-line notation in the same way as for plane figures.

For example, for the rotation in Figure 57, we have

$$\begin{pmatrix}1&2&3&4&5&6&7&8\\4&3&7&8&1&2&6&5\end{pmatrix}^{-1}=\begin{pmatrix}4&3&7&8&1&2&6&5\\1&2&3&4&5&6&7&8\end{pmatrix}$$
$$=\begin{pmatrix}1&2&3&4&5&6&7&8\\5&6&2&1&8&7&3&4\end{pmatrix}.$$

This is the rotation of the cube through $3\pi/2$ about the vertical line through the centre, in the direction indicated in Figure 60.

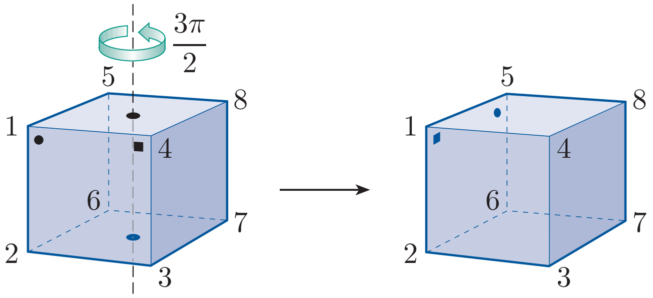


Figure 60 A rotation of the cube through $3\pi/2$ about its vertical axis

For any figure F, we denote the set of symmetries of F by $S(F)$. You saw earlier that if F is a plane figure, then $S(F)$ is a group under function composition. The arguments that confirmed this remain valid if F is a figure in $\mathbb{R}^3$, as you might like to check. So we have the following general result.

Theorem B21

If F is a figure (in $\mathbb{R}^2$ or $\mathbb{R}^3$), then $S(F)$ forms a group under function composition.

For any figure F, the group $(S(F), \circ)$ is called the **symmetry group**

Direct and indirect symmetries of a figure in $\mathbb{R}^3$

In Subsection 1.1 we demonstrated the symmetries of the square in $\mathbb{R}^2$ by using a paper model. You saw that we could demonstrate rotations of the square by moving the paper model within the plane, but that to demonstrate reflections we needed to 'flip' the paper square about an axis of symmetry.

For figures in $\mathbb{R}^3$, the only symmetries that we can demonstrate physically with a model are rotations. We cannot flip our model to demonstrate a reflection, as we did for the square – to do that, we would need access to a fourth dimension!

The symmetries of a figure in $\mathbb{R}^3$ that we can demonstrate with a model (that is, rotations) are called **direct** symmetries, whereas those that we cannot show physically with the model are called **indirect** symmetries.

For a polyhedron or any other figure in $\mathbb{R}^3$, we can imagine (or, if practicable, make) a *second* model to represent the reflected figure. You can think of this second model as the three-dimensional equivalent of the other side of a paper model of a plane figure, since the other side of the paper model is a model of the reflected plane figure. Earlier we shaded the model of the reflected plane figure a darker colour to distinguish it from the model of the original plane figure, and you might like to think of the model of the reflected figure in $\mathbb{R}^3$ as shaded darker too, to distinguish it from the original model.

As in the case of plane figures, composition of direct and indirect symmetries of figures in $\mathbb{R}^3$ follows a standard pattern, as follows.

$$\begin{aligned}\text{direct} \circ \text{direct} &= \text{direct}\\ \text{direct} \circ \text{indirect} &= \text{indirect}\\ \text{indirect} \circ \text{direct} &= \text{indirect}\\ \text{indirect} \circ \text{indirect} &= \text{direct}\end{aligned}$$

$\circ$	direct	indirect
direct	direct	indirect
indirect	indirect	direct

Also, as before, the inverse of a direct symmetry is a direct symmetry, and the inverse of an indirect symmetry is an indirect symmetry.

You also saw earlier that if F is a plane figure that has a finite number of symmetries, then either all the symmetries of F are direct symmetries, or half of the symmetries are direct and half are indirect. This is also true for figures in $\mathbb{R}^3$.

To see this, consider a figure F in $\mathbb{R}^3$, and suppose that it has n direct symmetries. In other words, there are n different ways to pick up a model of the figure and replace it to occupy the same space, but possibly with its vertices at different locations. If F has *no* indirect symmetries, then these n direct symmetries are the only symmetries of F. Now suppose that f has at least one indirect symmetry. This means that you can remove the model of F and replace it with the model of the reflected version of F, to occupy the same space. Once you have done that, there must be n different ways to pick up the reflected model again and replace it to occupy the same space. In other words, F has n indirect symmetries, and if you choose any one of them, then you can obtain all n of them by composing the one that you chose with each of the n direct symmetries in turn. (In other words, they can all be illustrated by rotating the second model of the polyhedron.)

So we have the following general result.

Theorem B22

If a figure (either a plane figure or a figure in $\mathbb{R}^3$) has a finite number of symmetries, then either

- all the symmetries are direct, or
- half of the symmetries are direct and half are indirect.

If there are indirect symmetries, then they can all be obtained by composing any single indirect symmetry with all of the direct symmetries.

We denote the set of direct symmetries of a figure F by $S^+(F)$.

5.2 Counting the symmetries of a polyhedron

Finding all the symmetries of a polyhedron is generally more tricky than finding all the symmetries of a plane figure such as a polygon. It is usually helpful to start by working out the *number of symmetries* that the polyhedron has. In this subsection you will see how to do this, and in the next subsection we will look at how you might go about actually finding the symmetries. We will start with the regular polyhedra.

Counting the symmetries of a regular polyhedron

As an example, let us try to count the symmetries of the simplest regular polyhedron, the tetrahedron, shown in Figure 61. In Figure 61, the lowest face of the tetrahedron is labelled as its *base*.

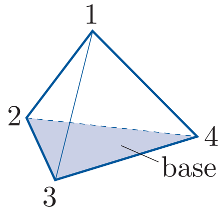


Figure 61 A tetrahedron

Imagine picking up the tetrahedron, and placing it down again to occupy the same space that it occupied originally, but possibly with the vertices at new locations. Let us count the number of ways of doing this. We can choose any of the four faces to be the base, and then there are three ways of placing the tetrahedron on this base, corresponding to the three rotational symmetries of the base triangle. Thus altogether there are $4 \times 3 = 12$ ways of placing the tetrahedron down again. Hence the tetrahedron has 12 direct symmetries. (One of them is the identity symmetry.)

The tetrahedron also has indirect symmetries – for example, a reflection in the vertical plane through the edge joining the vertices at locations 1 and 3 and the midpoint of the edge joining the vertices at locations 2 and 4, as shown in Figure 62.

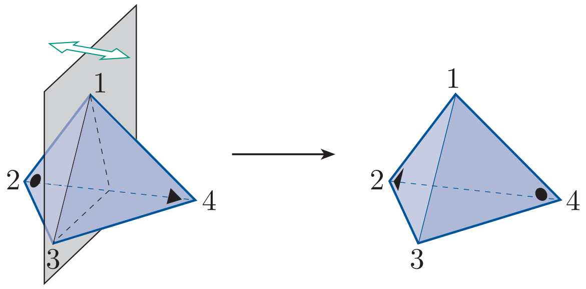


Figure 62 A reflectional symmetry of the tetrahedron

We know that if a figure with a finite number of symmetries has indirect symmetries, then it must have the same number of indirect symmetries as direct symmetries. It follows that the tetrahedron has 12 indirect symmetries, and hence it has 24 symmetries altogether.

Here is another way to work out that the tetrahedron has 24 symmetries. We count the number of ways of replacing the tetrahedron *or the reflected tetrahedron* in the space occupied originally by the tetrahedron, but possibly with the vertices at new locations. We can choose any of the four faces to be placed as the base. Now consider the symmetries of the base. It is an equilateral triangle, so it has six symmetries. Imagine applying any one of these symmetries to the base, and allowing the rest of the tetrahedron to be transformed accordingly. For example, if we rotate the base about its centre, then the whole tetrahedron is rotated about the vertical line through this point, as shown in Figure 63(a). Similarly, if we reflect the base in a line that goes through a vertex and the midpoint of the opposite edge, then the whole tetrahedron is reflected in the vertical plane that passes through this line, as shown in Figure 63(b). You can see that for each of the six symmetries of the base, the corresponding transformation, applied to the whole tetrahedron, results in the tetrahedron occupying the same space. Hence there are six ways of replacing the tetrahedron, or the reflected tetrahedron, on the base. Since there were four ways to choose the base, it follows that there are $4 \times 6 = 24$ symmetries of the tetrahedron.

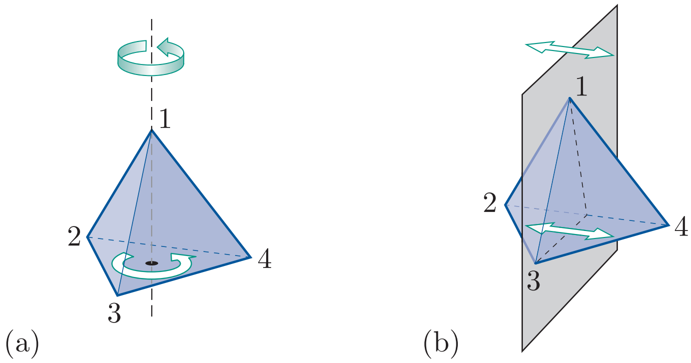


Figure 63 (a) Rotating the base and tetrahedron (b) Reflecting the base and tetrahedron

An argument similar to the one above holds for any regular polyhedron. In particular, once we have chosen a particular face to be the base, then for each symmetry of the base, the corresponding transformation applied to the whole polyhedron results in the polyhedron occupying the same space. It follows that the total number of symmetries of a regular polyhedron is the number of faces multiplied by the number of symmetries of each face. So we have the following strategy.

Strategy B1

To determine the number of symmetries of a regular polyhedron, do the following.

1. Count the number of faces.
2. Count the number of symmetries of a face.
3. Then

$$\begin{pmatrix}\text{number of}\\ \text{symmetries of the}\\ \text{regular polyhedron}\end{pmatrix} = \begin{pmatrix}\text{number of}\\ \text{faces}\end{pmatrix} \times \begin{pmatrix}\text{number of}\\ \text{symmetries of a face}\end{pmatrix}.$$

Exercise B31

Use Strategy B1 to show that the cube and the octahedron each have 48 symmetries, and that the dodecahedron and the icosahedron each have 120 symmetries.

(Remember that a regular n-gon has $2n$ symmetries, as described at the end of Subsection 1.1.)

Counting the symmetries of a non-regular polyhedron

Strategy B1 for determining the number of symmetries of a regular polyhedron can be adapted to allow us to find the number of symmetries of a non-regular polyhedron. To illustrate the method, let us consider two particular non-regular polyhedra.

First, we will look at the *pentagonal prism* shown in Figure 64, in which the top and bottom faces are regular pentagons, and the vertical faces are squares. (In general, a **prism** is a polyhedron two of whose faces are congruent, parallel polygons, and each of whose other faces is a parallelogram.)

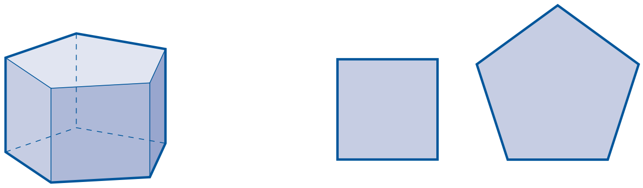


Figure 64 A pentagonal prism with square side faces, and its two face types

The pentagonal prism in Figure 64 has direct symmetries – for example, rotations about the vertical line through its centre, as shown in Figure 65(a). It also has indirect symmetries – for example, a reflection in a plane that contains a vertical edge of the prism and bisects the square face opposite this edge, as shown in Figure 65(b).

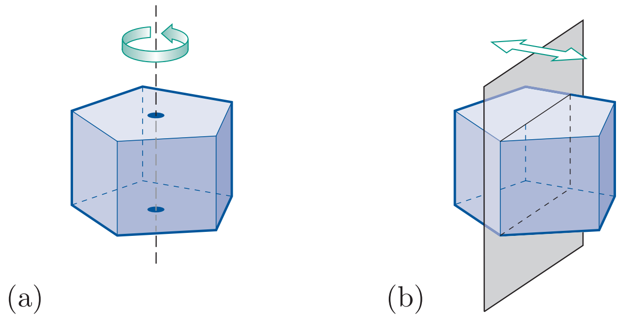


Figure 65 Rotational and reflectional symmetries of the pentagonal prism

To find the number of symmetries of the prism, we can count the number of ways of replacing the prism, or the reflected prism, in the space that it occupied originally, but possibly with the vertices at new locations.

In Figure 64, the prism is shown with a pentagonal face as its base, so we can choose either of the two pentagonal faces to be the base. The base has 10 symmetries, and we need to check whether, for each of these symmetries of the base, the corresponding transformation applied to the whole prism results in the prism occupying the same space. In other words, we need to check whether each of the 10 symmetries of the base gives a symmetry of the whole prism. You can see that this is indeed the case. So, for each of the two choices of base, there are 10 ways of replacing the prism, or the reflected prism, on the base. Thus there are $2 \times 10 = 20$ symmetries of the prism.

We carried out this calculation by considering one of the pentagonal faces as the base. We can check our answer by considering one of the square faces to be the base, as shown in Figure 66. This figure also indicates the shapes of the faces that share an edge with the square base.

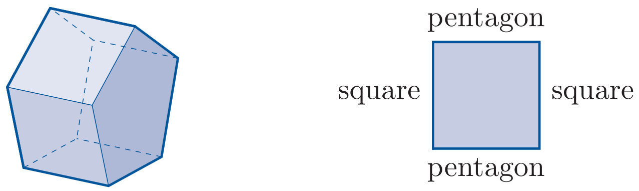


Figure 66 The prism with a square face as the base

Again we count the number of ways of replacing the prism, or the reflected prism, in the space that it originally occupied. We can choose any of the five square faces to be the base.

We now have to be careful because only some of the eight symmetries of the square base give symmetries of the whole prism. For example, one symmetry of the square base is a rotation of $\pi/2$ about its centre, but if we apply the corresponding transformation to the prism as a whole – that is, if we rotate the prism through $\pi/2$ about the vertical line through the centre of the square base, as shown in Figure 67 – then the prism does not occupy its original space in $\mathbb{R}^3$. So this transformation is not a symmetry of the prism. One way to see this is to observe that a symmetry of the square base that maps an edge joined to a pentagonal face to an edge joined to a square face cannot give a symmetry of the whole prism. Similarly, reflections through the diagonals of the square base do not give symmetries of the prism.

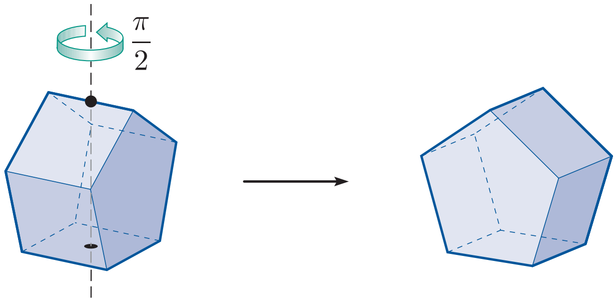


Figure 67 Rotation of the prism through $\pi/2$ about the vertical axis of symmetry

In fact, only four of the eight symmetries of the square base give symmetries of the prism, namely the identity, the rotation through π and the reflections in the lines joining the midpoints of opposite edges. Thus, since we can choose any of the five square faces to be the base, the number of symmetries of the prism is $5 \times 4 = 20$. This confirms our earlier answer.

Small rhombicuboctahedron

As a second example, we consider the polyhedron shown in Figure 68. It is called the **small rhombicuboctahedron**, and it has 18 square faces and 8 faces that are equilateral triangles. (It is not to be confused with the *great rhombicuboctahedron*, which has 12 square faces, 8 hexagonal faces and 6 octagonal faces.)

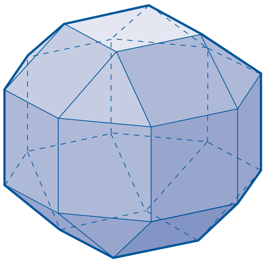


Figure 68 The small rhombicuboctahedron

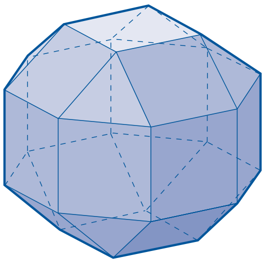


Figure 69 The small rhombicuboctahedron

To find the number of symmetries of the small rhombicuboctahedron, we can count the number of ways of replacing the polyhedron, or the reflected polyhedron, in the space that it occupied originally, as shown in Figure 69 with a square face as its base, but possibly with the vertices at new locations.

We immediately come across a new complication: only some of the square faces of the polyhedron can be placed as the base if the polyhedron, or its reflection, is to occupy its original space in $\mathbb{R}^3$. This is because there are two types of square face in the small rhombicuboctahedron. For one type, all four edges of the face are joined to other square faces, whereas for the other type, two edges are joined to square faces and two to triangular faces, as shown in Figure 70.

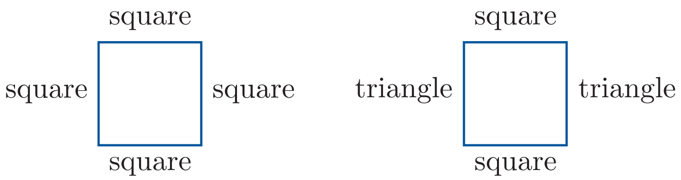


Figure 70 The two types of square face in the small rhombicuboctahedron

The small rhombicuboctahedron shown in Figure 69 has a square face of the first type as its base. There are six faces of this type in the polyhedron, and we can choose any of these to be placed as the base.

Next we have to determine how many of the eight symmetries of one of these square faces give symmetries of the polyhedron. Consideration of the polyhedron shows that all eight symmetries do, so the number of symmetries of the polyhedron is $6 \times 8 = 48$.

We could check this answer by taking one of the square faces of the second type, or one of the triangular faces, to be the base. In each case, we have to consider carefully how many symmetries of the base are symmetries of the whole polyhedron.

The two examples of counting the symmetries of a non-regular polyhedron that you have seen demonstrate the following general strategy.

Strategy B2

To determine the number of symmetries of a non-regular polyhedron, do the following.

1. Select one type of face.

   (For two faces to be of the same type, it must be possible to place the polyhedron with either of the faces as its base and have it occupy the same space.)

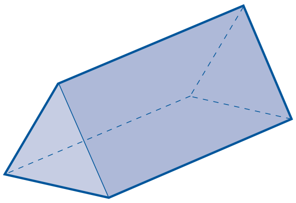
2. Count the number of faces of this type.
3. Count the symmetries of a face of this type that give symmetries of the polyhedron.

4. Then

$$\begin{pmatrix}\text{number of}\\ \text{symmetries of}\\ \text{the polyhedron}\end{pmatrix} = \begin{pmatrix}\text{number of}\\ \text{faces of the}\\ \text{selected type}\end{pmatrix} \times \begin{pmatrix}\text{number of}\\ \text{symmetries of a face}\\ \text{of this type that}\\ \text{give symmetries of}\\ \text{the polyhedron}\end{pmatrix}.$$

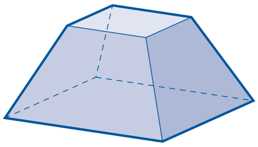
Exercise B32

Using Strategy B2, determine the number of symmetries of the triangular prism shown below. It has two faces that are equilateral triangles, and three faces that are non-square rectangles. Check your calculation by considering the solid in a different way.



Exercise B33

Determine the number of symmetries of the solid shown below, which has two square faces of different sizes, and four faces that are trapeziums with two equal edges.



In fact the symmetries of the solid in Exercise B33 are just the symmetries given by the eight symmetries of its square base, and hence it has eight symmetries. There are many solids whose symmetries are just the symmetries given by a related plane figure. For example, the symmetries of the hexagonal bottle in Figure 71 are the symmetries given by its hexagonal base, and hence it has 12 symmetries.

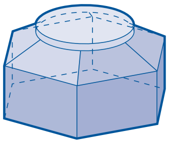


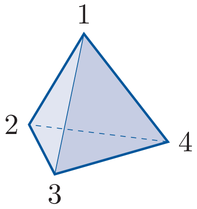
Figure 71 A hexagonal bottle

5.3 Finding the symmetries of a polyhedron

In this subsection you will see an example of how to actually find the symmetries of a polyhedron, once we know how many there are. The approach that we will take here allows us to describe the symmetries geometrically, as far as possible, as well as find their two-line symbols.

Worked Exercise B14

Find all the symmetries of the regular tetrahedron, shown below, describing them geometrically.



Solution

By Strategy B1, the tetrahedron has $4 \times 6 = 24$ symmetries (as found in the previous subsection). Since it has at least one indirect symmetry (such as reflection in the vertical plane that contains the edge joining locations 1 and 3), it has 12 direct symmetries and 12 indirect symmetries.

First we find the direct symmetries.

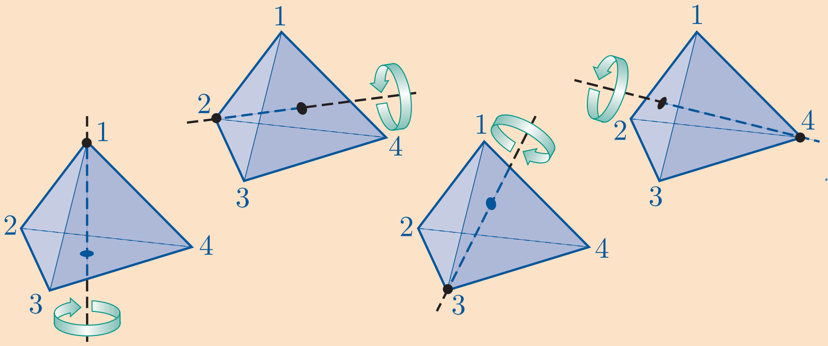
We always have the identity symmetry.

One direct symmetry is the identity symmetry,

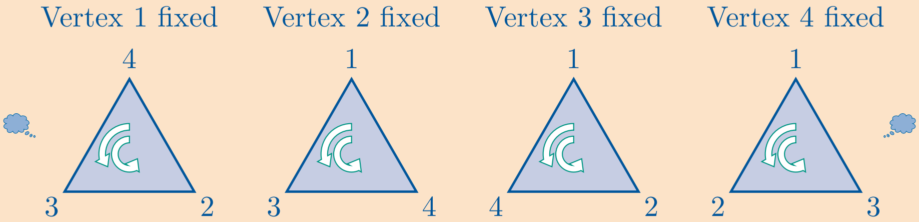
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}.$$

Look for non-trivial rotational symmetries.

For each vertex, there is an axis of symmetry that passes through the vertex and the centre of the opposite face.



A rotational symmetry about such an axis fixes the vertex that lies on the axis and rotates the opposite face.



There are two non-trivial rotational symmetries about each such axis, as follows.

The axis through the vertex at location 1 gives the rotations

$$\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\1&3&4&2\end{pmatrix}.$$

The axis through the vertex at location 2 gives the rotations

$$\begin{pmatrix}1&2&3&4\\3&2&4&1\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}.$$

The axis through the vertex at location 3 gives the rotations

$$\begin{pmatrix}1&2&3&4\\4&1&3&2\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\2&4&3&1\end{pmatrix}.$$

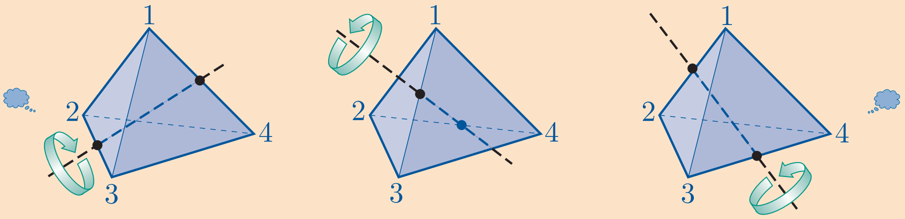
The axis through the vertex at location 4 gives the rotations

$$\begin{pmatrix}1&2&3&4\\2&3&1&4\end{pmatrix},\quad\begin{pmatrix}1&2&3&4\\3&1&2&4\end{pmatrix}.$$

We have now found nine direct symmetries, so there are three more. If we cannot spot them immediately, then we can try composing some of the direct symmetries found already, since a composite of direct symmetries is a direct symmetry. Composing the first and fourth non-trivial direct symmetries above gives

$$\begin{pmatrix}1&2&3&4\\4&2&1&3\end{pmatrix}\circ\begin{pmatrix}1&2&3&4\\1&4&2&3\end{pmatrix}=\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}.$$

This is a new direct symmetry. It interchanges the vertices at locations 1 and 4 and interchanges the vertices at locations 2 and 3. Geometrically, it is a rotation through π about the line through the midpoints of the opposite edges joining 1 to 4 and 2 to 3. There is a similar rotational symmetry for each of the other two pairs of opposite edges.

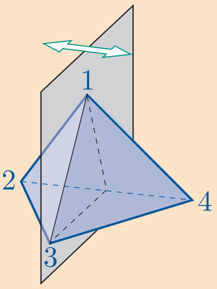


There are three rotations through axes of symmetry that join midpoints of opposite edges, as follows:

$$\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix},\quad \begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\quad \begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix}.$$

We have now found all 12 direct symmetries of the tetrahedron.

To find the indirect symmetries, find one reflectional symmetry, and compose it with all the direct symmetries already found (being consistent about whether the indirect symmetry is composed on the right or the left). An example of a reflectional symmetry is shown below.



One reflectional symmetry is reflection in the vertical plane through the edge joining the vertices at locations 1 and 3 and the midpoint of the edge joining the vertices at locations 2 and 4, that is,

$$\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix}.$$

Composing each of the 12 direct symmetries with this indirect symmetry on the right gives the following twelve indirect symmetries.

$$\begin{matrix}
\begin{pmatrix}1&2&3&4\\1&4&3&2\end{pmatrix} & \begin{pmatrix}1&2&3&4\\1&3&2&4\end{pmatrix} & \begin{pmatrix}1&2&3&4\\1&2&4&3\end{pmatrix} & \begin{pmatrix}1&2&3&4\\3&1&4&2\end{pmatrix}\\
\begin{pmatrix}1&2&3&4\\4&3&1&2\end{pmatrix} & \begin{pmatrix}1&2&3&4\\4&2&3&1\end{pmatrix} & \begin{pmatrix}1&2&3&4\\2&1&3&4\end{pmatrix} & \begin{pmatrix}1&2&3&4\\2&4&1&3\end{pmatrix}\\
\begin{pmatrix}1&2&3&4\\3&4&2&1\end{pmatrix} & \begin{pmatrix}1&2&3&4\\4&1&2&3\end{pmatrix} & \begin{pmatrix}1&2&3&4\\3&2&1&4\end{pmatrix} & \begin{pmatrix}1&2&3&4\\2&3&4&1\end{pmatrix}
\end{matrix}$$

Six of these indirect symmetries (the ones that fix two vertices and interchange two vertices) are reflections in a plane that passes through an edge and the midpoint of the opposite edge. There is one such reflectional symmetry for each of the six edges of the tetrahedron.

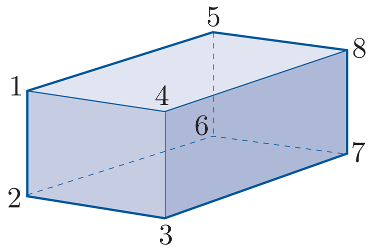
The remaining six indirect symmetries are not reflections, because the effect of a reflection on a point is to fix it (if it lies on the plane of reflection) or interchange it with another point (if it does not), and these six symmetries do not have that effect on the vertices. For example, the fourth indirect symmetry above maps the vertex at location 1 to the vertex at location 3, but it does not map the vertex at location 3 to the vertex at location 1.

The other six indirect symmetries do not have a simple geometric description: each of them is the composite of a reflection and a rotation.

In the worked exercise above it was mentioned that if a symmetry f is a reflection, then each point is either fixed by f or interchanged by f with another point. Note that the converse of this fact is not true: that is, a symmetry may have this effect on all points, but not be a reflection. For example, a rotation through π has this effect, as you will see in the next exercise.

Exercise B34

(a) Use Strategy B2 to show that the cuboid shown below has eight symmetries. Each of its faces is a non-square rectangle.



(b) Write down the two-line symbol for each of the eight symmetries, using the location labelling shown above.

You have seen that the set of symmetries of any figure in two- or three-dimensional space is a group under function composition. So, in particular, the 24 symmetries of the tetrahedron found in Worked Exercise B14 form a group under function composition, as do the eight symmetries of the cuboid found in Exercise B34. If we wished, we could construct the Cayley table for either of these groups by composing the elements using the two-line symbols for the symmetries. (For the tetrahedron, this would take rather a long time, and yield rather a large table!)

5.4 The Platonic solids

As you saw in Subsection 5.1, the Platonic solids are the convex polyhedra in which all the faces are congruent regular polygons and at each vertex the same number of faces meet, arranged in the same way. If you are interested in understanding why there are only five such solids, then read the explanation below. This material will not be assessed.

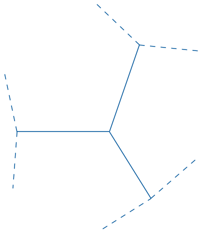


Figure 72 Three faces meeting at a vertex

Consider a solid of the description above. As for any solid, it must have at least three faces meeting at each vertex, as shown in Figure 72.

First suppose that the faces of the solid are equilateral triangles. There could be three, four or five equilateral triangles meeting at each vertex, as shown in Figure 73, but no more, as six equilateral triangles would lie flat, and more than six equilateral triangles would give a non-convex solid.

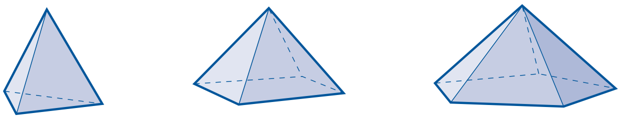


Figure 73 Three, four or five equilateral triangle faces meeting at a vertex

The arrangement of faces at each vertex of the solid must be the same, so we can build up the rest of the solid from the arrangement at one vertex. The three possibilities in Figure 73 give the tetrahedron, the octahedron and the icosahedron, respectively, as shown in Figure 74.

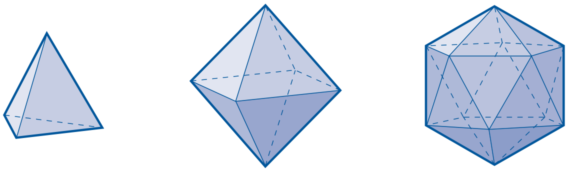


Figure 74 The regular tetrahedron, octahedron and icosahedron

Now suppose that the faces are not equilateral triangles, but squares. Three squares meeting at each vertex gives a cube. There cannot be more than three squares meeting at each vertex, because four squares would lie flat, and more than four squares would give a non-convex solid.

Next, suppose that the faces are regular pentagons. Three pentagons meeting at each vertex gives a dodecahedron. There cannot be more than three pentagons meeting at each vertex, as that would give a non-convex solid.

The cube and dodecahedron are shown in Figure 75.

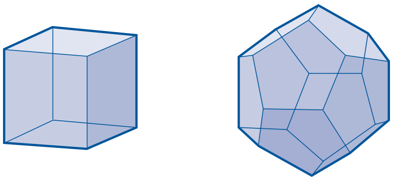


Figure 75 The cube and regular dodecahedron

There can be no more such solids, because three regular hexagons lie flat, and for any regular polygon with more than six edges, the angle at each vertex is greater than $2\pi/3$, so we cannot fit three together at a vertex without making the solid non-convex. (The angle at a vertex of a regular n-gon is $\pi - (2\pi/n)$, as shown in Figure 76, which is greater than $2\pi/3$ for $n > 6$.)

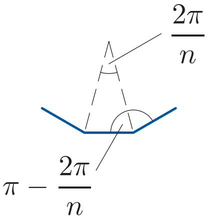


Figure 76 Angles in a regular n-gon

Thus there are precisely five regular polyhedra.

> The Greek mathematician Theaetetus (c.417–c.368 BCE) may have been the first to recognise that there are only five regular solids, and only a few years later Plato incorporated a discussion of Theaetetus' work in his own *Timaeus*. Book XIII of Euclid's *Elements* (c.300 BCE), which completely describes the regular solids, contains a proof that there are only five of them.

Summary

In this unit, you studied the symmetries of bounded figures in $\mathbb{R}^2$ and $\mathbb{R}^3$, and saw that composition of symmetries is closed and associative, that there is an identity symmetry and that every symmetry has an inverse. You saw that these properties are the group axioms, which are satisfied by other binary operations on sets in many areas of mathematics. Such a set with its binary operation is called a group, and if the binary operation is also commutative, the group is called abelian. You practised checking whether the group axioms hold, and met many examples of groups, including groups, both infinite and finite, whose elements are numbers and whose binary operation is addition, multiplication, modular addition or modular multiplication. You saw how to use the group axioms to deduce further properties that apply to all groups. For example, the identity and inverses in a group are unique, and the left and right cancellation laws always hold. In the remaining units in this book, you will see that we can say a great deal more about the structure of groups by making further deductions from the group axioms.

Learning outcomes

After working through this unit, you should be able to:

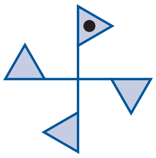
- explain what is meant by a *symmetry* of a figure in $\mathbb{R}^2$ or $\mathbb{R}^3$
- understand the difference between *direct* and *indirect* symmetries in $\mathbb{R}^2$ and $\mathbb{R}^3$
- find the symmetries of some bounded figures in $\mathbb{R}^2$ or $\mathbb{R}^3$ as *two-line symbols*, and describe them geometrically
- use two-line symbols to compose and invert symmetries
- explain the meaning of the terms *group*, *abelian* group and the *order* of a group
- determine whether a given set and *binary operation* form a group, by checking the group axioms
- construct a *Cayley table* for a finite set and binary operation, and use it to help you check the group axioms
- deduce information about a group from a *group table*
- be familiar with some standard types of groups, such as the groups formed by the symmetries of figures under function composition, groups of numbers under addition and multiplication, and groups from modular arithmetic
- know some basic properties of groups, such as that the identity in a group is unique and each element in a group has a unique inverse
- start to appreciate how some simple group properties can be proved by using the group axioms.

Solutions to exercises

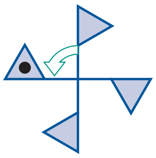
Solution to Exercise B1

(a) We can denote the initial position by a dot at the top.

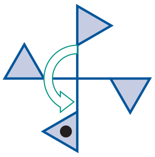
The symmetries are as follows.



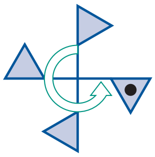
identity symmetry



rotation through $\pi/2$



rotation through π

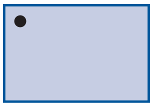


rotation through $3\pi/2$

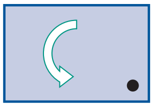
(There are no reflectional symmetries.)

(b) We can denote the initial position by a light colour and a dot in the top left corner, and think of a darker colour on the 'reverse'.

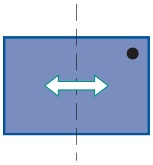
The symmetries are as follows.



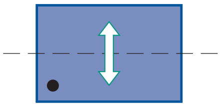
identity symmetry



rotation through π



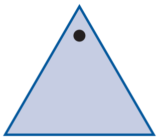
reflection in vertical



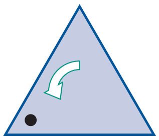
reflection in horizontal

(c) We can denote the initial position by a light colour and a dot in the top corner, and think of a darker colour on the 'reverse'.

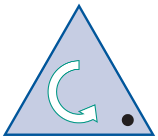
The symmetries are as follows.



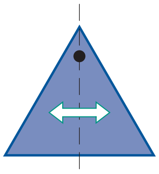
identity symmetry



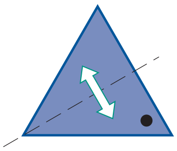
rotation through $2\pi/3$



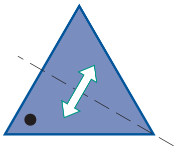
rotation through $4\pi/3$



reflection in vertical



reflection in slant axis

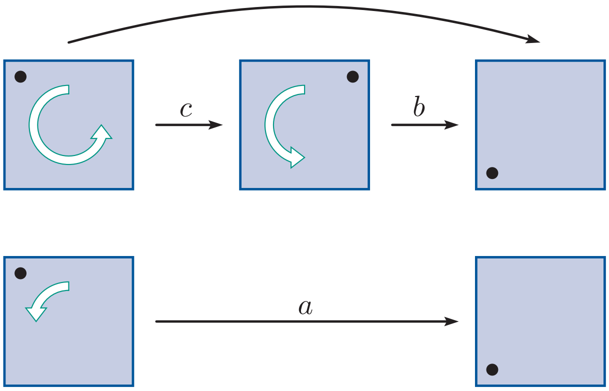


reflection in slant axis

Solution to Exercise B2

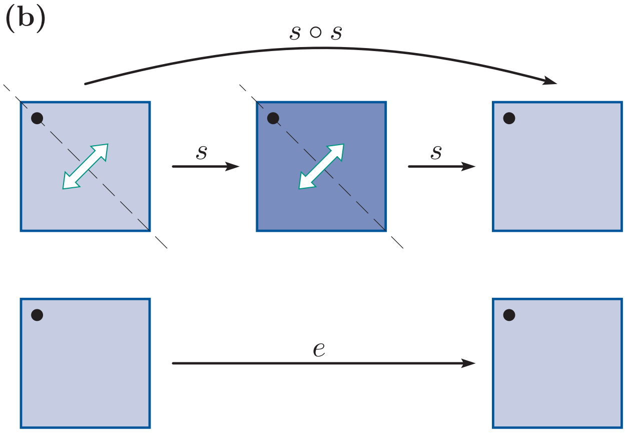
We find the required composites by drawing diagrams similar to those in Worked exercise B1.

(a)



Hence $b \circ c = a$.

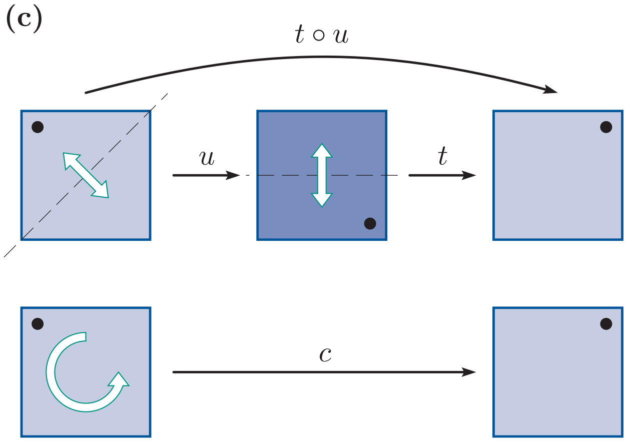
(b)



Hence $s \circ s = e$.

(Any reflection composed with itself is the same as the identity symmetry e.)

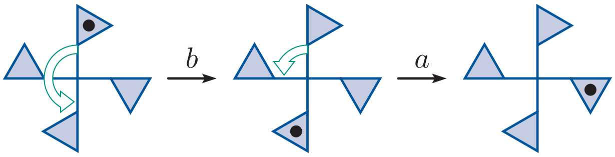
(c)



Hence $t \circ u = c$.

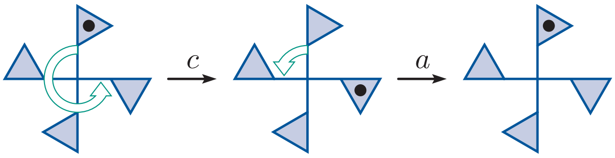
Solution to Exercise B3

(a) (i)



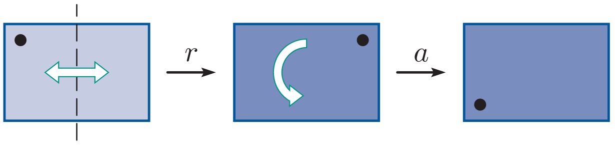
Hence $a \circ b = c$.

(ii)



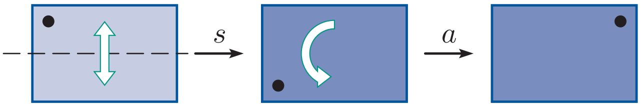
Hence $a \circ c = e$.

(b) (i)



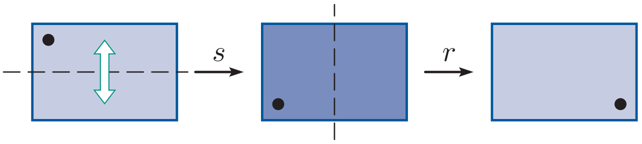
Hence $a \circ r = s$.

(ii)



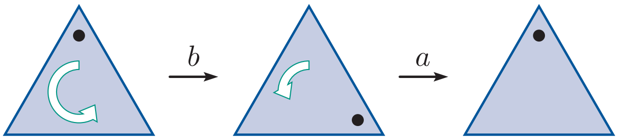
Hence $a \circ s = r$.

(iii)



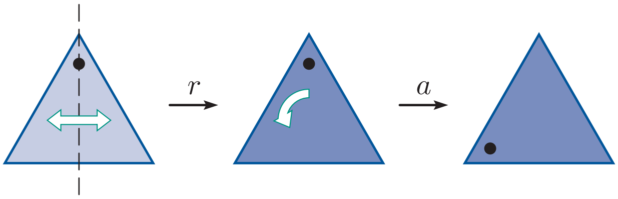
Hence $r \circ s = a$.

(c) (i)



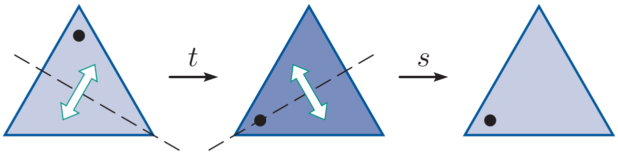
Hence $a \circ b = e$.

(ii)



Hence $a \circ r = t$.

(iii)



Hence $s \circ t = a$.

Solution to Exercise B4

We find the composites using the diagrammatic method demonstrated in Worked Exercise B1. (The diagrams are not given here.)

First we find $a \circ (t \circ a)$:

$$t \circ a = s \quad \text{and} \quad a \circ s = t,$$

so $a \circ (t \circ a) = t$.

Next we find $(a \circ t) \circ a$:

$$a \circ t = u \quad \text{and} \quad u \circ a = t,$$

so $(a \circ t) \circ a = t$.

Hence

$$a \circ (t \circ a) = (a \circ t) \circ a.$$

Solution to Exercise B5

(a) In S(✣), as in S(□), the rotations a and c are inverses of each other, and b is self-inverse.

Element	e	a	b	c
Inverse	e	c	b	a

(b) In S(▭), each element is self-inverse.

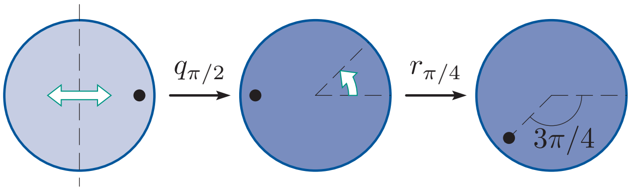
Element	e	a	r	s
Inverse	e	a	r	s

(c) In S(△), the rotations a and b are inverses of each other, and the other symmetries are self-inverse.

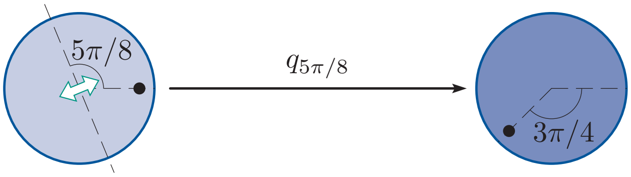
Element	e	a	b	r	s	t
Inverse	e	b	a	r	s	t

Solution to Exercise B6

We find $r_{\pi/4} \circ q_{\pi/2}$ using the following diagram.



Hence $r_{\pi/4} \circ q_{\pi/2} = q_{5\pi/8}$, as shown below.

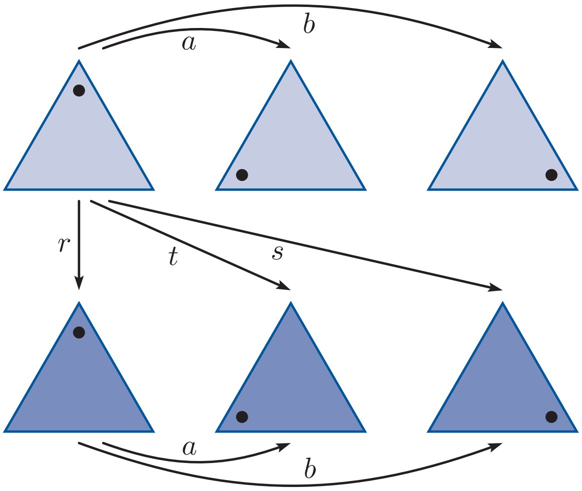


Solution to Exercise B7

(a) The set of direct symmetries of the equilateral triangle is

$$S^+(\triangle) = \{e, a, b\}.$$

Using the reflection r, we obtain the following diagram.



$r = e \circ r$ $\quad$ $t = a \circ r$ $\quad$ $s = b \circ r$

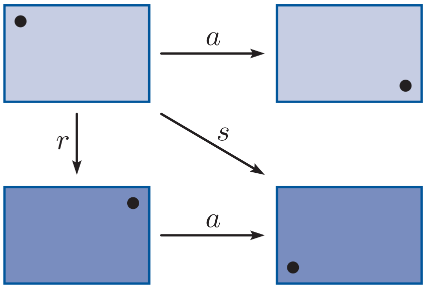
Instead of r, we could have used s or t as the reflection:

$$s = e \circ s, \quad r = a \circ s, \quad t = b \circ s,$$
$$t = e \circ t, \quad s = a \circ t, \quad r = b \circ t.$$

(b) The set of direct symmetries of the rectangle is

$$S^+(▭) = \{e, a\}.$$

Using the reflection r, we obtain the following diagram.



$r = e \circ r$ $\quad$ $s = a \circ r$

Alternatively, we could have used the reflection s:

$$s = e \circ s, \quad r = a \circ s.$$

Solution to Exercise B8

We have

$$b = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \quad c = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix},$$

$$s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}, \quad u = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}.$$

Solution to Exercise B9

Here

$$e = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

$$r = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}.$$

(Remember to include e.)

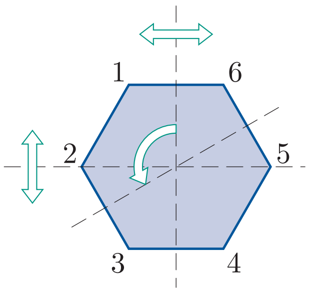
Solution to Exercise B10

We have

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix},$$

$$r = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}.$$

Solution to Exercise B11



(a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ represents reflection in the vertical axis of symmetry.

(b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$ represents anticlockwise rotation through $2\pi/3$ about the centre.

(c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 2 & 1 & 6 & 5 & 4 \end{pmatrix}$ represents reflection in the horizontal axis of symmetry.

Solution to Exercise B12

We have

$$a \circ a = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = b,$$

$$b \circ s = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = t,$$

$$s \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = r,$$

$$t \circ s = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = b.$$

Solution to Exercise B13

In each case we turn the two-line symbol upside down and reorder the columns.

(a)
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 1 & 2 & 3 & 4 \end{pmatrix}^{-1} = \begin{pmatrix} 5 & 6 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 6 & 1 & 2 \end{pmatrix}$$

(b)
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 2 & 1 & 6 & 5 & 4 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 1 & 6 & 5 & 4 & 3 \end{pmatrix}$$

(c)
$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 4 & 5 & 6 & 1 & 2 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 6 & 1 & 2 & 3 \end{pmatrix}$$

Solution to Exercise B14

We have

$$b \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = a,$$

$$b \circ t = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = r,$$

$$t \circ b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = s,$$

$$t \circ t = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e.$$

Thus the Cayley table for $S(\triangle)$ is as follows.

$\circ$	e	a	b	r	s	t
e	e	a	b	r	s	t
a	a	b	e	t	r	s
b	b	e	a	s	t	r
r	r	s	t	e	a	b
s	s	t	r	b	e	a
t	t	r	s	a	b	e

Solution to Exercise B15

The symmetry a is a half-turn, so $a \circ a = e$.

The symmetry s is a reflection, so $s \circ s = e$.

Also,

$$\begin{aligned} a \circ s &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = r, \end{aligned}$$

and

$$\begin{aligned} s \circ a &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} = r. \end{aligned}$$

Thus the Cayley table for S(▭) is as follows.

$\circ$	e	a	r	s
e	e	a	r	s
a	a	e	s	r
r	r	s	e	a
s	s	r	a	e

Solution to Exercise B16

(a) We check the group axioms for $(\mathbb{Z}, +)$. The arguments are similar to those in Worked Exercise B7.

G1 For all $m, n \in \mathbb{Z}$,

$$m + n \in \mathbb{Z},$$

since the sum of two integers is an integer. So $\mathbb{Z}$ is closed under addition.

G2 Addition of integers is associative.

G3 We have $0 \in \mathbb{Z}$, and for all $n \in \mathbb{Z}$,

$$n + 0 = n = 0 + n.$$

So 0 is an identity element for addition on $\mathbb{Z}$.

G4 For each $n \in \mathbb{Z}$, we have $-n \in \mathbb{Z}$, and

$$n + (-n) = 0 = (-n) + n,$$

so $-n$ is an inverse of n.

Thus each element of $\mathbb{Z}$ has an inverse in $\mathbb{Z}$ with respect to addition.

Hence $(\mathbb{Z}, +)$ satisfies the four group axioms, and so is a group.

(b) We check the group axioms for $(\mathbb{Q}^*, \times)$. The arguments are similar to those in Worked Exercise B8.

G1 Let $x, y \in \mathbb{Q}^*$. Then $x \times y \in \mathbb{Q}$, since the product of two rational numbers is a rational number. Also $x \times y \neq 0$, since $x \neq 0$ and $y \neq 0$. Hence

$$x \times y \in \mathbb{Q}^*,$$

so $\mathbb{Q}^*$ is closed under multiplication.

G2 Multiplication of rational numbers is associative.

G3 We have $1 \in \mathbb{Q}^*$, and for all $x \in \mathbb{Q}^*$,

$$x \times 1 = x = 1 \times x.$$

So 1 is an identity element for multiplication on $\mathbb{Q}^*$.

G4 Let $x \in \mathbb{Q}^*$. Then $x \neq 0$, so $1/x$ exists, and lies in $\mathbb{Q}^*$, since the reciprocal of a non-zero rational number is a non-zero rational number. Also

$$x \times \frac{1}{x} = 1 = \frac{1}{x} \times x.$$

Hence $1/x$ is an inverse of x.

Thus each element of $\mathbb{Q}^*$ has an inverse in $\mathbb{Q}^*$ with respect to multiplication.

Hence $(\mathbb{Q}^*, \times)$ satisfies the four group axioms, and so is a group.

Solution to Exercise B17

(a) The set $\mathbb{Q}$ is closed under multiplication; multiplication of rational numbers is associative; and 1 is a multiplicative identity in $\mathbb{Q}$, so axioms G1, G2 and G3 hold.

However, axiom G4 fails, because 0 has no multiplicative inverse in $\mathbb{Q}$.

Hence $(\mathbb{Q}, \times)$ is not a group.

(b) The sum of two positive real numbers is a positive real number, so $\mathbb{R}^+$ is closed under addition. Also, addition of real numbers is associative. So axioms G1 and G2 hold.

However, axiom G3 fails: there is no identity element. This is because, for example, there is no element $e \in \mathbb{R}^+$ such that

$$2 + e = 2,$$

since $0 \notin \mathbb{R}^+$.

Hence $(\mathbb{R}^+, +)$ is not a group.

(c) The product of two odd integers is odd, so D is closed under multiplication. Multiplication of integers is associative. Also, 1 is odd, so 1 is a multiplicative identity in D. So axioms G1, G2 and G3 hold.

However, axiom G4 fails because, for example, 3 has no multiplicative inverse in D, since $\frac{1}{3} \notin D$.

Hence $(D, \times)$ is not a group.

(d) We show that the four group axioms hold.

G1 If m and n are even numbers, then $m+n$ is an even number, so E is closed under $+$.

G2 Addition of numbers is associative.

G3 We have $0 \in E$ (since 0 is even), and for all $n \in E$,

$$n + 0 = n = 0 + n,$$

so 0 is an identity element for $+$ on E.

G4 For each even number n, the number $-n$ is also even, and

$$n + (-n) = 0 = (-n) + n,$$

so $-n$ is an inverse of n.

Hence $(E, +)$ satisfies the four group axioms, and so is a group.

(e) The set E is closed under subtraction, so axiom G1 holds.

However, axiom G2 (associativity) fails. For example, the numbers 6, 4 and 2 belong to E, and

$$6 - (4 - 2) = 6 - 2 = 4,$$

but

$$(6 - 4) - 2 = 2 - 2 = 0.$$

Since $4 \neq 0$, subtraction is not associative on E.

Hence $(E, -)$ is not a group.

Alternatively, we can show that axiom G3 (identity) fails. There is no identity element, since, for example, there is no even integer n such that

$$2 - n = 2 = n - 2.$$

(f) The numbers -1 and -2 lie in M, but

$$(-1) \times (-2) = 2 \notin M.$$

So M is not closed under $\times$. That is, axiom G1 fails.

Solution to Exercise B18

The approach is similar to that in Worked Exercise B11.

An identity element $e \in \mathbb{R}$ must have the property that, for each $x \in \mathbb{R}$,

$$x \circ e = x = e \circ x.$$

The equation $x \circ e = x$ gives

$$x - e - 1 = x,$$

which gives

$$e = -1.$$

So the only possibility for an identity element is $e = -1$.

However, if $e = -1$, then

$$e \circ x = -1 \circ x = -1 - x - 1 = -2 - x,$$

and $-2 - x$ is not equal to x in general, because, for example, taking $x = 0$ gives $-2 - x = -2 \neq 0$.

So -1 is not an identity element for $(\mathbb{R}, \circ)$, and hence there is no identity element.

That is, axiom G3 fails.

Hence $(\mathbb{R}, \circ)$ is not a group.

(Note that axiom G2 (associativity) also fails for the set $\mathbb{R}$ with this binary operation.)

Solution to Exercise B19

(a) Let $x, y, z \in \mathbb{R}$. Then

$$\begin{aligned}
&x \circ (y \circ z) \\
&= x \circ (y + z - yz) \\
&= x + (y + z - yz) - x(y + z - yz) \\
&= x + y + z - xy - xz - yz + xyz
\end{aligned}$$

and

$$\begin{aligned}
&(x \circ y) \circ z \\
&= (x + y - xy) \circ z \\
&= (x + y - xy) + z - (x + y - xy)z \\
&= x + y + z - xy - xz - yz + xyz.
\end{aligned}$$

The two expressions obtained are the same, so $\circ$ is associative on $\mathbb{R}$.

(b) Let $x, y, z \in \mathbb{R}$. Then

$$\begin{aligned} & x \circ (y \circ z) \\ &= x \circ (y - z + yz) \\ &= x - (y - z + yz) + x(y - z + yz) \\ &= x - y + z + xy - xz - yz + xyz \end{aligned}$$

and

$$\begin{aligned} & (x \circ y) \circ z \\ &= (x - y + xy) \circ z \\ &= (x - y + xy) - z + (x - y + xy)z \\ &= x - y - z + xy + xz - yz + xyz. \end{aligned}$$

The two expressions obtained are not equivalent.

For example, if $x = 0$, $y = 1$ and $z = 2$, then

$$\begin{aligned} 0 \circ (1 \circ 2) &= 0 \circ (1 - 2 + 2) \\ &= 0 \circ 1 \\ &= 0 - 1 + 0 = -1 \end{aligned}$$

but

$$\begin{aligned} (0 \circ 1) \circ 2 &= (0 - 1 + 0) \circ 2 \\ &= (-1) \circ 2 \\ &= -1 - 2 - 2 = -5. \end{aligned}$$

So $\circ$ is not associative.

(If you can see that a binary operation $\circ$ is not associative, then you do not need to find the general expressions for $x \circ (y \circ z)$ and $(x \circ y) \circ z$. It is enough to give a specific counterexample to demonstrate that $\circ$ is not associative.)

Solution to Exercise B20

We show that the four group axioms hold.

G1 For all $a, b \in \mathbb{Q}^+$, we have $a \circ b = \frac{1}{2}ab \in \mathbb{Q}^+$, so $\mathbb{Q}^+$ is closed under $\circ$.

G2 For all $a, b, c \in \mathbb{Q}^+$,

$$\begin{aligned} a \circ (b \circ c) &= a \circ \left(\tfrac{1}{2}bc\right) \\ &= \tfrac{1}{2}a(\tfrac{1}{2}bc) \\ &= \tfrac{1}{4}abc \end{aligned}$$

and

$$\begin{aligned} (a \circ b) \circ c &= \left(\tfrac{1}{2}ab\right) \circ c \\ &= \tfrac{1}{2}(\tfrac{1}{2}ab)c \\ &= \tfrac{1}{4}abc. \end{aligned}$$

The two expressions obtained are the same, so $\circ$ is associative on $\mathbb{Q}^+$.

G3 We try to find a likely candidate for the identity. We seek an element $e \in \mathbb{Q}^+$ such that, for all $a \in \mathbb{Q}^+$,

$$a \circ e = a = e \circ a.$$

The equation $a \circ e = a$ gives

$$\tfrac{1}{2}ae = a,$$

which gives $e = 2$.

Now $2 \in \mathbb{Q}^+$, and for all $a \in \mathbb{Q}^+$,

$$a \circ 2 = \tfrac{1}{2} \times a \times 2 = a$$

and

$$2 \circ a = \tfrac{1}{2} \times 2 \times a = a.$$

So 2 is indeed an identity element for $(\mathbb{Q}^+, \circ)$.

G4 Let $a \in \mathbb{Q}^+$. An inverse of a is not obvious, so we try to find a likely candidate. We seek an element $x \in \mathbb{Q}^+$ such that

$$a \circ x = 2 = x \circ a.$$

The equation $a \circ x = 2$ gives $\frac{1}{2}ax = 2$ and hence $x = 4/a$, so the only possibility for an inverse of a is $4/a$.

Now $4/a \in \mathbb{Q}^+$, and

$$a \circ \frac{4}{a} = \frac{1}{2} \times a \times \frac{4}{a} = 2$$

and

$$\frac{4}{a} \circ a = \frac{1}{2} \times \frac{4}{a} \times a = 2.$$

So $4/a$ is an inverse of a.

Hence $(\mathbb{Q}^+, \circ)$ satisfies the four group axioms, and so is a group.

Solution to Exercise B21

(a) This situation is similar to that in Worked Exercise B12.

The Cayley table for $(\mathbb{Z}_5, +_5)$ is as follows.

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

We show that the four group axioms hold.

G1 All the elements in the table are in $\mathbb{Z}_5$, so $\mathbb{Z}_5$ is closed under $+_5$.

G2 The operation $+_5$ is associative.

G3 The row and column labelled 0 repeat the table borders, so 0 is an identity element.

G4 From the Cayley table, we see that

$$0 +_5 0 = 0,$$
$$1 +_5 4 = 0 = 4 +_5 1,$$
$$2 +_5 3 = 0 = 3 +_5 2,$$

so

0 is self-inverse,

1 and 4 are inverses of each other,

2 and 3 are inverses of each other.

Hence $(\mathbb{Z}_5, +_5)$ satisfies the four group axioms, and so is a group.

(b) This situation is similar to that in Worked Exercise B13.

The Cayley table for $(\mathbb{Z}_5, \times_5)$ is as follows.

$\times_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Axioms G1, G2 and G3 hold, and 1 is an identity element.

However, there is no 1 in the row labelled 0, so 0 has no inverse and therefore axiom G4 fails.

Hence $(\mathbb{Z}_5, \times_5)$ is not a group.

(c) In this case, the troublesome 0 in part (b) has been omitted, and the Cayley table is as follows.

$\times_5$	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

We check the four group axioms in turn.

G1 All the elements in the table are in $\{1, 2, 3, 4\}$, so $\{1, 2, 3, 4\}$ is closed under $\times_5$.

G2 The operation $\times_5$ is associative.

G3 The row and column labelled 1 repeat the table borders, so 1 is an identity element.

G4 From the table, we see that

$$1 \times_5 1 = 1,$$
$$4 \times_5 4 = 1,$$
$$2 \times_5 3 = 1 = 3 \times_5 2,$$

so

1 and 4 are self-inverse,

2 and 3 are inverses of each other.

Hence $(\{1, 2, 3, 4\}, \times_5)$ satisfies the four group axioms, and so is a group.

(d) The Cayley table for $(\{1, 2, 3, 4, 5\}, \times_6)$ is as follows.

$\times_6$	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

The body of the table contains occurrences of the number 0, which is not an element of $\{1, 2, 3, 4, 5\}$, so axiom G1 fails.

Hence $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group.

(Another way to show that $(\{1, 2, 3, 4, 5\}, \times_6)$ is not a group is to show that axiom G4 fails. The number 1 is an identity element for $(\{1, 2, 3, 4, 5\}, \times_6)$, but there is no 1 in the row labelled 2, so 2 has no inverse.)

(e) The Cayley table for $(\{2, 4, 6, 8\}, \times_{10})$ is as follows.

$\times_{10}$	2	4	6	8
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

We check the four group axioms in turn.

G1 All the elements in the table are in $\{2, 4, 6, 8\}$, so $\{2, 4, 6, 8\}$ is closed under $\times_{10}$.

G2 The operation $\times_{10}$ is associative.

G3 The row and column labelled 6 repeat the table borders, so 6 is an identity element.

G4 From the table, we see that

$$4 \times_{10} 4 = 6,$$
$$6 \times_{10} 6 = 6,$$
$$2 \times_{10} 8 = 6 = 8 \times_{10} 2,$$

so

4 and 6 are self-inverse,

2 and 8 are inverses of each other.

Hence $(\{2,4,6,8\},\times_{10})$ satisfies the four group axioms, and so is a group.

(f) The Cayley table for $(\{1,-1\},\times)$ is as follows.

$\times$	1	-1
1	1	-1
-1	-1	1

We check the four group axioms in turn.

G1 All the elements in the table are in $\{1,-1\}$, so this set is closed under ×.

G2 Multiplication of numbers is associative.

G3 From the table, we see that 1 is an identity element.

G4 Since $1\times 1=1$ and $(-1)\times(-1)=1$, the elements 1 and -1 are both self-inverse.

Hence $(\{1,-1\},\times)$ satisfies the four group axioms, and so is a group.

Solution to Exercise B22

We check the four group axioms in turn.

G1 All the elements in the table are in $\{a,b,c,d,e,f,g,h\}$, so this set is closed under $\circ$.

G2 We are told that the operation $\circ$ is associative.

G3 The row and column labelled e repeat the table borders, so e is an identity element.

G4 From the table, we see that

$$a\circ b=e=b\circ a,$$
$$c\circ d=e=d\circ c,$$
$$e\circ e=e,$$
$$f\circ f=e,$$
$$g\circ h=e=h\circ g,$$

so

e and f are self-inverse,

a and b are inverses of each other,

c and d are inverses of each other,

g and h are inverses of each other.

Hence $(\{a,b,c,d,e,f,g,h\},\circ)$ satisfies the four group axioms, and so is a group.

Solution to Exercise B23

(a) A Cayley table for $(\mathbb{Z}_7,+_7)$ is

$+_7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

The inverses of the elements are as follows.

Element	0	1	2	3	4	5	6
Inverse	0	6	5	4	3	2	1

(b) A Cayley table for $(\mathbb{Z}_7^*,\times_7)$ is

$\times_7$	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

The inverses of the elements are as follows.

Element	1	2	3	4	5	6
Inverse	1	4	5	2	3	6

(c) We have

$$U_{10}=\{1,3,7,9\}.$$

A Cayley table for $(U_{10},\times_{10})$ is

$\times_{10}$	1	3	7	9
1	1	3	7	9
3	3	9	1	7
7	7	1	9	3
9	9	7	3	1

The inverses of the elements are as follows.

Element	1	3	7	9
Inverse	1	7	3	9

(d) We have

$$U_9 = \{1, 2, 4, 5, 7, 8\}.$$

A Cayley table for $(U_9, \times_9)$ is

$\times_9$	1	2	4	5	7	8
1	1	2	4	5	7	8
2	2	4	8	1	5	7
4	4	8	7	2	1	5
5	5	1	2	7	8	4
7	7	5	1	8	4	2
8	8	7	5	4	2	1

The inverses of the elements are as follows.

Element	1	2	4	5	7	8
Inverse	1	5	7	2	4	8

Solution to Exercise B24

Suppose that, in a group $(G, \circ)$,

$$a \circ x = b \circ x.$$

Composing both sides on the right with the inverse of x, we obtain

$$a \circ x \circ x^{-1} = b \circ x \circ x^{-1}.$$

By axiom G2 (associativity), this gives

$$a \circ (x \circ x^{-1}) = b \circ (x \circ x^{-1}).$$

Hence, by axiom G4 (inverses), we obtain

$$a \circ e = b \circ e,$$

and therefore, by axiom G3 (identity),

$$a = b.$$

Solution to Exercise B25

We know that

$$a \circ b \circ c = e.$$

Composing both sides on the left with the inverse of a gives

$$a^{-1} \circ a \circ b \circ c = a^{-1} \circ e.$$

By axiom G2 (associativity), this gives

$$(a^{-1} \circ a) \circ b \circ c = a^{-1} \circ e.$$

Hence, by axiom G4 (inverses), we obtain

$$e \circ b \circ c = a^{-1} \circ e,$$

and therefore, by axiom G3 (identity),

$$b \circ c = a^{-1}.$$

Now composing both sides on the right by a gives

$$b \circ c \circ a = a^{-1} \circ a.$$

Hence, by axiom G4 (inverses), we obtain

$$b \circ c \circ a = e,$$

as required.

Solution to Exercise B26

First we prove the 'if' part. Suppose that $(G, \circ)$ is abelian. We have to show that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G.$$

So let $x, y \in G$. Then

$$\begin{aligned} &(x \circ y)^{-1} \\ &= y^{-1} \circ x^{-1} \quad \text{(by Proposition B14)} \\ &= x^{-1} \circ y^{-1} \quad \text{(since } (G, \circ) \text{ is abelian).} \end{aligned}$$

This proves the required statement.

Now we prove the 'only if' part. Suppose that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G.$$

We have to show that $(G, \circ)$ is abelian. Let $x, y \in G$. Then

$$\begin{aligned} &x \circ y \\ &= ((x \circ y)^{-1})^{-1} \quad \text{(by Proposition B13)} \\ &= (x^{-1} \circ y^{-1})^{-1} \\ &\qquad \text{(by the supposition above)} \\ &= (y^{-1})^{-1} \circ (x^{-1})^{-1} \quad \text{(by Proposition B14)} \\ &= y \circ x \quad \text{(by Proposition B13).} \end{aligned}$$

This shows that $(G, \circ)$ is abelian, and completes the required proof.

(There are many different ways to prove the 'only if' part here. Here is another way to do it. Suppose that

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1} \text{ for all } x, y \in G.$$

We have to show that $(G, \circ)$ is abelian. Let $x, y \in G$.

By the supposition above, we have

$$(x \circ y)^{-1} = x^{-1} \circ y^{-1},$$

and by Proposition B14, we have

$$(x \circ y)^{-1} = y^{-1} \circ x^{-1}.$$

Hence

$$x^{-1} \circ y^{-1} = y^{-1} \circ x^{-1}.$$

Composing both sides on the left and right by x gives

$$x \circ x^{-1} \circ y^{-1} \circ x = x \circ y^{-1} \circ x^{-1} \circ x,$$

that is, by axiom G4,

$$e \circ y^{-1} \circ x = x \circ y^{-1} \circ e,$$

which gives, by axiom G3,

$$y^{-1} \circ x = x \circ y^{-1}.$$

Now composing both sides on the left and right by y gives

$$y \circ y^{-1} \circ x \circ y = y \circ x \circ y^{-1} \circ y,$$

that is, by axiom G4,

$$e \circ x \circ y = y \circ x \circ e,$$

which gives, by axiom G3,

$$x \circ y = y \circ x.$$

Hence $(G, \circ)$ is abelian.)

Solution to Exercise B27

(a) The second row and the second column repeat the borders of the table, so the identity is E.

(b) The first row and the first column repeat the borders of the table, so the identity is D.

(c) The third row and the third column repeat the borders of the table, so the identity is w.

Solution to Exercise B28

Let g be any group element; we will consider the column corresponding to g. Let h also be any group element; we will show that h occurs exactly once in this column.

This is equivalent to proving that there is *exactly one* element of the group, x say, such that

$$x \circ g = h,$$

as illustrated below.

$$\begin{array}{c|ccc} & \cdots & g & \cdots \\ \hline \vdots & & \vdots & \\ x & \cdots & h & \cdots \\ \vdots & & \vdots & \end{array}$$

To show that there is *at least* one such element x, let $x = h \circ g^{-1}$. Then

$$\begin{aligned} x \circ g &= h \circ g^{-1} \circ g \\ &= h \circ e \\ &= h, \end{aligned}$$

so $x = h \circ g^{-1}$ has the property $x \circ g = h$, as claimed.

To show that $x = h \circ g^{-1}$ is the *only* element x of the group such that $x \circ g = h$, suppose that x and y are group elements such that

$$x \circ g = h \quad \text{and} \quad y \circ g = h.$$

Then

$$x \circ g = y \circ g,$$

so, by the Right Cancellation Law,

$$x = y.$$

So there is indeed exactly one element x of the group such that $x \circ g = h$, namely $x = h \circ g^{-1}$.

In other words, in the column labelled g, the element h appears exactly once; it appears in the row labelled by the element $h \circ g^{-1}$.

Solution to Exercise B29

(a) The element e does not appear symmetrically with respect to the main diagonal, so the Cayley table is not a group table.

Alternatively, the elements a, b and c do not have inverses. For example, from the row labelled a we see that the only possible candidate for a^{-1} is c, since $a \circ c = e$; but from the row labelled c we see that $c \circ a = d \neq e$, so a has no inverse.

(b) The element d occurs twice in the row labelled b (and also twice in the column labelled b), so the Cayley table is not a group table.

Solution to Exercise B30

(a) The group table is symmetric with respect to the main diagonal, so this group is abelian.

The table of inverses is as follows.

Element	e	a	b	c	d	f	g	h
Inverse	e	a	b	c	d	f	g	h

(b) The group is non-abelian; for example, $a \circ d = f$, but $d \circ a = h$.

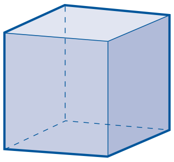
The table of inverses is as follows.

Element	e	a	b	c	d	f	g	h
Inverse	e	c	b	a	g	h	d	f

Solution to Exercise B31

In each case, we use Strategy B1.

Cube

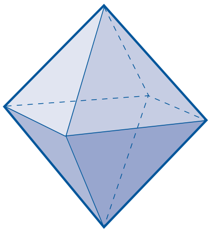


The cube has six faces.

Each face of the cube is a square, and so has eight symmetries (since the order of $S(\square)$ is 8).

It follows from the strategy that the number of symmetries of the cube is 6 × 8 = 48.

Octahedron

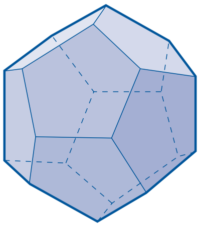


The octahedron has eight faces.

Each face of the octahedron is an equilateral triangle, and so has six symmetries (since the order of $S(\triangle)$ is 6).

It follows from the strategy that the number of symmetries of the octahedron is $8 \times 6 = 48$.

Dodecahedron

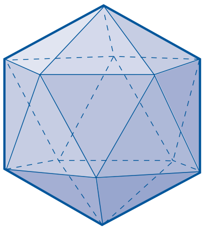


The dodecahedron has 12 faces.

Each face of the dodecahedron is a regular pentagon, and so has 10 symmetries (since the order of $S(⬠)$, the symmetry group of the regular pentagon, is 10).

It follows from the strategy that the number of symmetries of the dodecahedron is $12 \times 10 = 120$.

Icosahedron



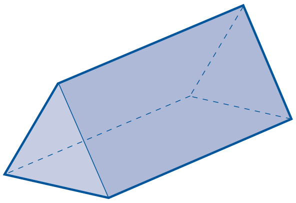
The icosahedron has 20 faces.

Each face of the icosahedron is an equilateral triangle, and so has six symmetries.

It follows from the strategy that the number of symmetries of the icosahedron is $20 \times 6 = 120$.

Solution to Exercise B32

We use Strategy B2.



The triangular prism has two (congruent) equilateral triangle faces and three (congruent) rectangular faces, so there are two ways of applying the strategy.

Consider the equilateral triangle faces.

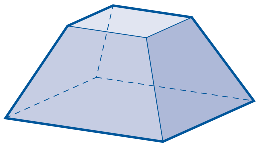
1. The prism has two equilateral triangle faces.
2. Each of the six symmetries of a face of this type gives a symmetry of the whole prism.
3. Hence the number of symmetries of the triangular prism is $2 \times 6 = 12$.

Alternatively, consider the rectangular faces.

1. The prism has three rectangular faces.
2. Each of the four symmetries of a face of this type gives a symmetry of the whole prism.
3. Hence the number of symmetries of the triangular prism is $3 \times 4 = 12$.

Solution to Exercise B33

We can use Strategy B2.



Consider one of the square faces, say the larger one.

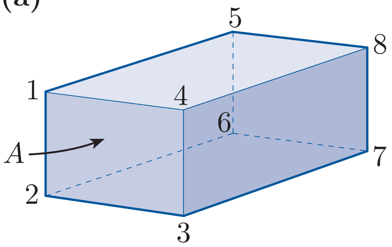
1. The solid has one face of this type.
2. Each of the eight symmetries of this face gives a symmetry of the whole solid.
3. Hence the number of symmetries of the solid is $1 \times 8 = 8$.

Alternatively, consider the trapezium faces.

1. The solid has four trapezium faces.
2. Each trapezium face has two symmetries (the identity and a reflection). Each of these two symmetries gives a symmetry of the whole solid.
3. Hence the number of symmetries of the solid is $4 \times 2 = 8$.

Solution to Exercise B34

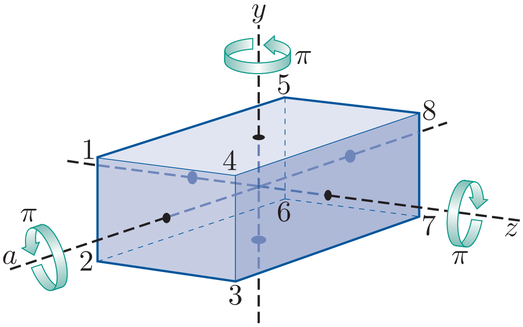
(a)



We use Strategy B2 to count the number of symmetries of the cuboid. The cuboid has six faces – three pairs of opposite faces. Opposite faces are congruent rectangles, and adjacent faces are not congruent. We choose one pair of opposite faces.

1. The cuboid has two faces of the type denoted by A in the diagram above.
2. Each of these faces is a rectangle, and so has four symmetries. Each of these symmetries gives a symmetry of the whole cuboid.
3. Hence the number of symmetries of the cuboid is $2 \times 4 = 8$.

(b) The cuboid has indirect symmetries, so it has four direct symmetries and four indirect symmetries. We first find the direct symmetries. The non-trivial direct symmetries are the rotations a, y and z through π about the axes shown below.



The two-line symbols for the direct symmetries are

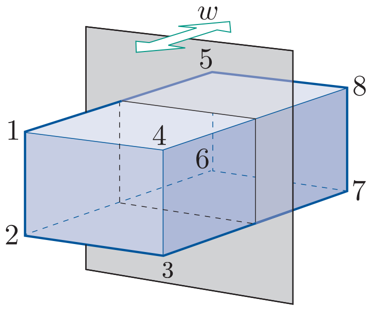
$$e = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \end{pmatrix},$$

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 4 & 1 & 2 & 7 & 8 & 5 & 6 \end{pmatrix},$$

$$y = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 8 & 7 & 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix},$$

$$z = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 5 & 8 & 7 & 2 & 1 & 4 & 3 \end{pmatrix}.$$

We can obtain the four indirect symmetries by composing each of these direct symmetries with the reflectional symmetry w in the vertical plane shown below.



This symmetry is

$$w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix},$$

so the four indirect symmetries are

$$w = e \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 5 & 6 & 7 & 8 & 1 & 2 & 3 & 4 \end{pmatrix},$$

$$x = a \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 8 & 5 & 6 & 3 & 4 & 1 & 2 \end{pmatrix},$$

$$r = y \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 2 & 1 & 8 & 7 & 6 & 5 \end{pmatrix},$$

$$s = z \circ w = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 2 & 1 & 4 & 3 & 6 & 5 & 8 & 7 \end{pmatrix}.$$

(Three of these four indirect symmetries, namely w, r and s, are reflections in a plane parallel to a pair of opposite faces. Although the other indirect symmetry, x, interchanges pairs of points, it is not a reflection in a plane. It is the composite of a rotational symmetry and a reflection in a plane.)